

2. Azaola, Elena: El delito de ser mujer, 2<sup>a</sup> ed., 2001, México: Plaza and Valdés – Centro de Investigaciones y Estudios Superiores en Antropología Social.

3. Badr-Eldin-Ali: “Female criminality in modern Egypt: A general outlook” in International Journal of Comparative and Applied Criminal Justice 21, 1997. - Pp. 267-286.

4. Carlen, Pat: “Criminal women and criminal justice, the limits to, and potential of, feminist and left realist perspectives” in J. Young and R. Mathews edtrs., Issues in realist criminology, 1992, London: Sage.

**Мазур Марина Іванівна,**  
курсантка 3-го курсу ННІ № 3  
Національної академії внутрішніх справ  
Консультант з мови: **Шемякіна Н. В.**  
доцент кафедри правничої лінгвістики,  
кандидат філологічних наук, доцент

## **LE DISPOSITIF NATIONAL DE LUTTE CONTRE LA CYBERCRIMINALITÉ EN FRANCE ET EN UKRAINE**

La société connaît aujourd’hui une phase de transformation numérique de grande ampleur et l’ensemble de nos systèmes sont de plus en plus interconnectés [1]. Attaques informatiques contre les systèmes d’information d’entreprises ou d’institutions, vols de bases de données afin d’obtenir une rançon, espionnage, financement d’organisations terroristes par du crowdfunding, escroqueries en ligne : la délinquance a investi l’espace cyber. Les menaces peuvent provenir d’Etats, d’entreprises privées ou d’organisations criminelles. Certaines opérations relèvent d’une nouvelle forme de cybercriminalité organisée. Aussi, les attaques informatiques ne constituent plus un simple risque conjoncturel, mais sont devenues systémiques, comme l’ont démontré les attaques[1].

La cybercriminalité est l’une des formes de la criminalité qui connaît la plus forte croissance tant au niveau national qu’international. Elle recouvre ainsi toute activité illégale ou irrégulière réalisée à travers le cyberspace: escroqueries, fraudes, extorsions, abus, espionnages, vandalismes etc. La cybercriminalité comprend toute forme de malveillance électronique effectuée au moyen de l’informatique et des télécommunications (téléphonie, cartes bleue etc)[2].

En droit français, la cybercriminalité est définie comme l’ensemble des infractions pénales qui sont commises via les réseaux informatiques, notamment, sur le réseau Internet. Ce terme désigne à la fois:

1) les atteintes aux biens: fraude à la carte bleue sur Internet sans le consentement de son titulaire; vente par petites annonces ou aux enchères d’objets volés ou contrefaits; encaissement d’un paiement sans livraison de la marchandise ou autres escroqueries en tout genre; piratage d’ordinateur; gravure pour soi ou pour autrui de musiques, films ou logiciels.

2) les atteintes aux personnes: diffusion d'images pédophiles, de méthodes pour se suicider, de recettes d'explosifs ou d'injures à caractère racial; diffusion auprès des enfants de photographies à caractère pornographique ou violent; atteinte à la vie privée [4].

Pour lutter contre ce phénomène, en France le décret du 15 mai 2000 a créé au sein de la direction centrale de la police judiciaire un office central de la lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC).

OCLCTIC est chargé:

1) d'animer et coordonner la lutte contre les auteurs d'infractions liées aux technologies de l'information et de la communication;

2) de procéder, à la demande de l'autorité judiciaire, à tous actes d'enquêtes et travaux techniques d'investigations;

3) d'apporter, à leur demande, une assistance aux services de police, de gendarmerie et de douane en cas d'infractions liées aux hautes technologies;

4) de centraliser et diffuser l'information sur les infractions technologiques à l'ensemble des services répressifs.

L'OCLCTIC traite les affaires judiciaires qui concernent les atteintes aux systèmes de traitements automatisés de données, les fraudes aux télécommunications, les fraudes aux cartes de paiement et à microprocesseurs, ainsi que toutes les formes de criminalité qui utilisent les nouvelles technologies. En fonction des nécessités, l'office peut effectuer une surveillance active des réseaux (site web, forum de discussions...) et procéder à toute vérification utile ainsi qu'à la localisation de serveurs[4].

En Ukraine, la cyberpolice a été créée le 5 octobre 2015. C'est un office territorial interrégional de la police nationale de l'Ukraine qui fait partie de la police criminelle et, conformément à la législation ukrainienne, assure la mise en œuvre de la politique d'État dans la lutte contre la cybercriminalité. Elle est chargée de: la prévention, la repression et la détection des infractions pénales ainsi que des mécanismes de préparation, commission ou dissimulation d'une infraction en utilisant le réseau et systèmes informatiques Internet. Les missions de la cyberpolice ukrainienne sont suivantes :

1) mettre en œuvre la politique de l'État dans le domaine de la lutte contre la cybercriminalité;

2) informer rapidement la population de l'apparition des nouvelles formes de la cybercriminalité;

3) mettre en place un logiciel d'analyse et d'information sur des cyberincidents, des cybermenaces et des cybercrimes;

4) répondre aux demandes des partenaires étrangers via le réseau national de points de contact 24h / 24;

5) assurer la formation des policiers ukrainiens dans le domaine de la lutte contre la cybercriminalité;

6) participer aux opérations internationales et coopérer en temps réel en matière de la lutte contre la cybercriminalité.

7) lutter contre la cybercriminalité [3].

Donc, pour lutter contre la cybercriminalité il existe un dispositif spécial national et international. En France la lutte contre la cybercriminalité est assurée par l'Office central de la lutte contre la criminalité liée aux technologies de l'information et de la communication, en Ukraine, par la cyberpolice.

Je pense que la meilleure façon de la lutte contre la cybercriminalité est de prendre des mesures préventives et d'être vigilant parce que ces dernières années, la démocratisation de l'accès aux ordinateurs et la mondialisation des réseaux sont devenues des facteurs de développement de la cybercriminalité. Aussi le Conseil de l'Europe aide à protéger les sociétés contre les menaces de la cybercriminalité par la biais de la Convention sur la cybercriminalité et son Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, le Comité de la Convention sur la Cybercriminalité et les programmes de coopération sur la cybercriminalité.

#### **Список використаних джерел:**

1. Nicolas Arpagian, Cybercriminalité : un rapport propose de créer le «police-secours» de l'internet, Le Journal du Net, 1<sup>er</sup> juillet 2014.

2. La lutte contre la cybercriminalité: la France au cœur du concert européen. – Christian Aghroum- <https://doi.org/10.3917/secug.006.0035>.

3. La cybercriminalité – <https://fr.wikipedia.org/wiki/>. – La lutte contre la cybercriminalité.

4. Шемякіна Н. В. Французька мова для працівників правоохоронних органів [Мультимедійний навч. посіб.] / Шемякіна Н. В. – Київ: МВС України. НАВС – 2020. [Електронний ресурс] Режим доступу до ресурсу: <https://arm.naiu.kiev.ua/books/french/index.html#>

**Майстренко Анастасія Олександрівна,**  
курсантка 2-го курсу ННІ № 3  
Національної академії внутрішніх справ  
Науковий керівник: **Козубенко І. В.**  
викладач кафедри правничої лінгвістики

#### **CONTRACTUALIZATION IN THE FIELD OF CRIME PREVENTION IN FRANCE**

Since the early 1980s, the implementation of crime prevention policies in France has rested on local coordination mechanisms and contract procedures between communities and the State, approaches that have been based on territoriality and partnerships. In tandem with the development of urban policy, this approach, promoted by the State, is closely linked to the process of decentralization and the progressive strengthening of the mayor's leadership role in