5. Facebook Newsroom (2016). Company Info. http://newsroom.fb.com/company-info

6. Lovejoy, Ben (2018). 'Tim Cook meets with Chinese vice premier in Beijing following iCloud phishing attack', http://www.techgreatest.com/apple-news/tim-cook-meets-withchinese-vice-premier-in-beijing-following-icloud-phishingattack/.

7. Brodkin, Jon (2011). 'Ballmer to Hu: 90% of Microsoft customers in China using pirated software', http://www.networkworld.com/article/2199038/software/ballmer-to-hu--90--of-microsoft-customers-in-china-using-piratedsoftware.html

Добридень Г.,
курсант Національної академії внутрішніх справ
Консультант з мови: **Шемякіна Н.В.**

LA LUTTE CONTRE LA CYBERCRIMINALITÉ EN FRANCE

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. [1]

La cybercriminalité se développe considérablement dans le monde de la technologie. Les criminels du World Wide Web exploitent les informations personnelles des internautes à leur avantage. Ils utilisent allègrement le dark web pour acheter et vendre des produits et des services illégaux. Ils réussissent même à avoir accès à des informations classifiées du gouvernement.[2,5]

Il faut souligner que les premiers cas de cybercriminalité ont eu lieu avant même qu'Internet n'existe et étaient liés … au vol de données. Les ordinateurs, les réseaux informatiques et Internet ont été conçus pour la création, le stockage et le transfert d'informations gouvernementales et de données d'entreprise, des informations très utiles pour les individus ayant de bonnes intentions. La création de méthodes numérisées peut avoir aidé l'humanité à se développer au 21ème siècle, mais cela a produit les mêmes effets pour les criminels. Ces derniers veulent ce que nous avons et plus nous essayons de dissimuler ces informations, de les rendre compliquées à récupérer et à exploiter et plus ils ont envie d'y accéder. Pas forcément pour en tirer profit, parfois juste pour prouver qu'ils peuvent y avoir accès. [2,5]

La cybercriminalité se divise en trois grandes catégories : la cybercriminalité individuelle, la cybercriminalité contre la propriété et la cybercriminalité gouvernementale. Les types de méthodes utilisées et les niveaux de difficulté varient selon la catégorie. Cela signifie que la cybercriminalité a instauré une menace majeure pour les utilisateurs

d'Internet, des millions d'informations utilisateur ayant été volées ces dernières années. Il a également eu un impact énorme sur l'économie de nombreux pays. [6]

Le crime se cache juste en dessous de la surface d'Internet. Il agit comme un champignon que vous ne pouvez pas voir, en diffusant sur le web les cyberattaques. La raison pour laquelle il est capable de se répandre ainsi est lié à un certain nombre de facteurs. Tout d'abord, les criminels peuvent facilement se cacher derrière leurs terminaux loin des régulateurs, opérant ainsi en toute impunité en utilisant les derniers logiciels de haute technologie. Deuxièmement, Internet offre un accès facile à presque tous sur la planète . Troisièmement, si on veut lancer une cyber arnaque, il ne faut pas être programmeur. Il suffit de savoir où la victime peut en trouver un à payer.[3]

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

- d'animer et coordonner la lutte contre les auteurs d'infractions liées aux technologies de l'information et de la communication;
- de procéder, à la demande de l'autorité judiciaire, à tous actes d'enquêtes et travaux techniques d'investigations;
- d'apporter, à leur demande, une assistance aux services de police, de gendarmerie et de douane en cas d'infractions liées aux hautes technologies;
- de centraliser et diffuser l'information sur les infractions technologiques à l'ensemble des services répressifs.[4]

On peut en déduire que compte tenu des innombrables techniques qu'emploient les cybercriminels pour s'attaquer aux ordinateurs et aux données des utilisateurs, des défenses multicouches sont nécessaires. Les solutions de protection contre les programmes malveillants qui allient la détection basée sur les signatures, l'analyse heuristique et les nouvelles technologies permettent de renforcer la protection des ordinateurs, appareils et données contre les menaces toujours plus sophistiquées.[6]

Список використаних джерел

1. Шемякіна Н.В. «Французька мова для правоохоронців» https://arm.naiau.kiev.ua/books/french/

2. Cybercriminalité. www.gouvernement.fr

3. D'où vient la cybercriminalité ? les origines et l'évolution de la cybercriminalité. www.le-vpn.com/fr

4. Lutte contre la cybercriminalité. https://www.police-nationale.interieur.gouv.fr

5. Quels sont les différents types de cybercriminalité? https://www.pandasecurity.com
6. Qu'est-ce que la cybercriminalité: définition. https://www.kaspersky.fr

Дяченко М.,
курсант Національної академії внутрішніх справ
Консультант з мови: **Романов І.І.**

COMBATING CRIME IN CANADA

What is organized crime? Under the *Criminal Code* (Section 467.1), organized crime is defined as being composed of three or more persons, having as one of its main purposes a serious offence likely to result in a financial benefit. So, just about any type of illicit activity can be undertaken by organized crime groups, as long as there is money to be made. Identity theft, human trafficking, sex crimes against children, credit card fraud and counterfeit goods, just to name a few, can, and often do have links to organized crime.

Plans and Priorities. The RCMP is created to safe homes and safe communities for all Canadians, and to accomplish this we identified the fight against organized crime as a strategic priority in 2001. Using an intelligence-led, integrated approach, the RCMP is focusing its activities on reducing the threat and impact of organized crime. In fulfilling its mandate, the RCMP is working closely with domestic and international partners in a sustained effort to dismantle today's criminal groups. To contribute to a successful outcome, the RCMP will:

- reduce the total harmful effects caused by organized crime by disrupting illicit markets;
- improve the quality of the criminal intelligence/information process;
- share intelligence with partners and cooperate with enforcement units at the municipal, national and international levels;
- formulate an up-to-date picture of the threat of organized crime and prioritize investigations;
- provide scientific and technical support and new technologies to enhance investigative abilities;
- enhance public awareness of the dangers and impacts of organized crime;
- reduce demand for illicit products [1].