Netherlands), fall within the top six highest juvenile prison populations – with the notable exception of the Netherlands which has only recently developed harsher penal policies.

Список використаних джерел

1. Goldson Barry and Muncie John, Youth Crime and Justice [Electronic resources] Available at : https://books.google.com.ua/books?id=p0ICzKfYnJQC&pg=PA78&hl=uk&source=gbs_toc_r&cad=3#v=onepage&q&f (last visited November 8, 2018).

2. Muncie John, Youth and Crime [Electronic resources] Available at : https://books.google.com.ua/books?id=hr8bmUVxaswC&pg=PA88&hl=uk&source=gbs_toc_r&cad=3#v=onepage&q&f (last visited November 8, 2018).

3. UNICEF, The State of the World's Children 1998 [Electronic resources] Available at : https://www.unicef.org/sowc98/ (last visited November 8, 2018).

Толочко О., Чабан К.,
курсанти ННІ № 2 Національної академії внутрішніх справ
Консультант з мови: **Василенко О.В.**

FIGHTING CYBER CRIMINAL ACTIVITY IN THE USA

Cybercrime is the fastest growing type of criminal activity in the United States – and it's affecting more and more of us each year! Whether it's credit card fraud, identity theft, email hacking, account stealing or any other number of activities – you're in the midst of an online war you may not even know it. Billions of dollars are spent each year combating cybercrime and yet the number, intensity and severity of attacks keeps increasing. Cybercrime is especially troubling for people who want to build their own website [1].

Cybercrime refers to any crime involving computers, mobile devices or Internet services. The FBI investigates computer crimes, which often cross borders and therefore pose jurisdictional problems for law enforcement officers. Crimes fall into two general categories: crimes made possible by computer networks and crimes that target computers directly.

Crimes that use networks include the following offenses: phishing scams; malware and viruses; denial of service for malicious mischief; identity theft and fraud; information theft; cyber talking.

Computer crime involves both hardware and software, and the Department of Justice classifies cybercrime in three ways.

1. Criminals target the computer. These crimes could include theft of data, viruses, or hardware theft.

2. Computers act as weapons to commit crimes. Criminals use computers and technology to commit many kinds of traditional crime.

3. Computers act as legal accessories, storing incriminating information [2].

Cybercrime is on the rise in America, with more than 143 million Americans affected by cybercrime in 2017, according to the Norton Cyber Security Insights Report. Nearly 8 in 10 US consumers surveyed reported themselves or someone they know being victimized, so it's understandable that Americans are worried more about cybercrimes than other crimes. Cybercrime costs have surpassed the expenses caused by black market sales of marijuana, heroin and cocaine combined. Symantec, a major security service, estimates that direct crime costs companies $114 billion annually, but the costs of recovery from cybercrimes add another $274 billion.

The U.S. Justice Department prosecutes computer crimes under *three different sections* of federal law.

First, there is the Computer Fraud and Abuse Act of 1986 (CFAA), codified in 18 U.S.C. Sec. 1030, covers nine different offenses whose maximum statutory penalties range from one year to life imprisonment. These offenses and maximum penalties include:

- obtaining National Security Information: 10 years for first offense, 20 years second offense;
- accessing a Computer and Obtaining Information: 1 or 5 years for first offenses, 10 years second offense;
- trespassing in a Government Computer: 1 year for first offense; 10 years second offense;
- accessing a Computer to Defraud & Obtain Value: 5 years for first offense, 10 years second offense;
- intentionally Damaging by Knowing Transmission: 1 or 10 years for first offense, 20 years second offense;
- recklessly damaging by Intentional Access: 1 or 5 years for first offense, 20 years second offense;
- negligently Causing Damage & Loss by Intentional Access: 1 year for first offense, 10 years for second offense;
- trafficking in Passwords: 1 year for first offense, 10 years second offense;
- extortion Involving Computers: 5 years for first offense, 10 years for second offense.

Second, the Wiretap Act, also known as “Title III,” involves the use of wiretaps while investigating crime. This Act prohibits “any person,” including a law enforcement officer, from making an illegal interception or disclosing or using illegally intercepted material. This Act covers three different offenses codified in 18 U.S.C. Sec. 2511: intercepting Communications; disclosing an Intercepted Communication; using an Intercepted Communication.

Third, is a catchall of what is known as other Network Crime Statutes. These statutes all have their own penalties and fines depending upon the circumstances under which the offense is committed: unlawful Access to Stored Communications: 18 U.S.C. Sec. 2701; identity Theft: 18 U.S.C. Sec. 1028; aggravated Identity Theft: 18 U.S.C. Sec. 1028A; access Device Fraud: 18 U.S.C. Sec. 1029; CAN-SPAM Act: 18 U.S.C. Sec. 1037; wire Fraud: 18 U.S.C. Sec. 1343.

Nearly 50 percent of Americans don't use antivirus software. The survey of people's internet habits across the United States was presented some very common (and very risky) online behaviors include: not using antivirus software; sharing your account passwords; using too-simple passwords, or reusing the same password for multiple accounts; not using an ad or pop-up blocker; opening emails, clicking links, and downloading files from unknown sources; not installing security on mobile devices [4].

Researches provides some tips to help avoid cybercrime such as:

1. Malware : Install an Internet security suite on all your devices, including your PCs, Macs, tablets and smartphones.
2. Debit or credit card fraud : Sign up for a credit monitoring service that can alert you to any unusual card activity.
3. Data breaches : Sign up for an identity theft protection service that can monitor for and alert you to any suspicious activity, such as credit card applications using your personally identifiable information.
4. Compromised passwords : Create strong, complicated passwords that are hard to crack. Use a combination of 10 numbers, upper and lowercase letters, and symbols — or consider using a password manager.
5. Unauthorized email and social media access : The best defense for these types of accounts is also a strong password. Avoid the temptation to use the same password for each account, and then take the time to craft a super strong password. Remember, your email and social media accounts can be used as credentials to access your other accounts, so guard them carefully and never share [3].

Список використаних джерел

1. Cybercrime In America – Which State Is Most At Risk In 2018? URL : <https://www.websitebuilderexpert.com /us-state-cybercrime-losses/>

2. Cybercrime Laws In The United States. URL : <http://www.aaronkellylaw.com/cybercrime-laws-united-states/>

3. Cybercrimes in America. Cyber security insights report. URL : <https://us.norton.com/internetsecurity-online-scams-top-5-cybercrimes-in-america-norton-cyber-security-insights-report.html>

4. The riskiest states for cybercrime in America. URL : <https://www.webroot.com/blog/2018/06/05/2018-riskiest-states-for-cybercrime-in-america/>

Торбич О.,
курсант ННІ 1 Національної академії внутрішніх справ
Консультант з мови: **Драмарецька Л.Б.**

FRENCH POLICY ON CYBERSECURITY

In recent years, France has completely reformulated its defense and national security priorities, taking into account the increase in volume, level, intensity and complexity of cyber-threats, including cybercrime, political and economic espionage. The White Paper on National Defense and Security 2008 was the first fundamental document devoted only to the problem of national cyber threats as a risk for national security and sovereignty. It defines new priorities, such as prevention and response to cyber-attacks, and institutional changes needed to ensure national security.

In accordance with the recommendations of the "White Paper" in 2008, one of the three bodies, directly subordinate to the Prime Minister - the Secretariat General of National Defense (General Secretariat of Defense Nationale, SGDN) was renamed General of Defense and the Secretariat National Security Council (General Secretariat for Defense and Security National, SGDSN). These changes led to the enlargement of powers of the Secretariat - to provide conventional defense with armed forces - to the wider responsibilities of the security of the whole society in cases beyond the need to use only military forces by traditional or security agencies.

These larger powers reflected the need to protect society in newer times, more complex and more turbulent, especially given the probability increasing cyber-crimes committed by adversaries of the enemy state or non-systemic. In 2009, the General Directorate of Computer Security (DCSSI) has been transformed into the National Security Systems Agency information system (National Agency for Information Systems Security, ANSSI), and is now the body responsible for the safety of national information systems.