

of bullying, its consequences and the possibility of providing qualified psychological assistance to the child [5].

Список використаних джерел:

1. Anti bullying week resources and information: [Електронний ресурс] – Режим доступу <https://www.bullying.co.uk/anti-bullying-week/>
2. Bullying: A review of the evidence [Електронний ресурс] – Режим доступу <https://epi.org.uk/publications-and-research/bullying-a-review-of-the-evidence/>
3. Bullying in UK Schools [Електронний ресурс] – Режим доступу <https://researchbriefings.files.parliament.uk/documents/CBP-8812/CBP-8812.pdf>
4. Information and Support: Bullying [Електронний ресурс] – Режим доступу <https://www.bbc.co.uk/programmes/articles/5Ffpz77jVbLvjsFj9GvKd8l/information-and-support-bullying>
5. Bullying [Електронний ресурс] – Режим доступу <https://learnenglishteens.britishcouncil.org/uk-now/read-uk/bullying>

Дячук Н.,

здобувач ступеня вищої освіти бакалавра
Національної академії внутрішніх справ

Консультант з мови: Хоменко О.

CURRENT STATE OF CYBER SECURITY IN USA

According to an official website of the United States government about cybersecurity & infrastructure security agency (CISA), cyberspace and its underlying infrastructure are vulnerable to a wide range of risks stemming from both physical and cyber threats and hazards. There are enough cyber actors and nation-states who exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services [1].

Particularly, cyberspace is difficult to secure due to a number of factors:

- 1) The ability of malicious actors to operate from anywhere in the world;
- 2) The linkages between cyberspace and physical systems;
- 3) The difficulty of reducing vulnerabilities and consequences in complex cyber networks.

Of growing concern is the cyber threat to critical infrastructure, which is increasingly subject to sophisticated cyber intrusions that pose new risks. As information technology becomes increasingly integrated with

physical infrastructure operations, there is increased risk for wide scale or high-consequence events that could cause harm or disrupt services upon which economy of USA and the daily lives of millions of Americans depend. In light of the risk and potential consequences of cyber events, strengthening the security and resilience of cyberspace has become an important homeland security mission [2].

Cyberspace is an integral component of all facets of American life, including the country's economy and defense. Yet private and public entities still struggle to secure their systems, and adversaries have increased the frequency and sophistication of their malicious cyber activities.

In partnership with other countries, the Department of State is leading the U.S. government's efforts to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation [2].

In nowadays, President Biden has made cybersecurity, a critical element of the Department of Homeland Security's (DHS) mission, a top priority for the Biden-Harris Administration at all levels of government.

To advance the President's commitment, and to reflect that enhancing the nation's cybersecurity resilience is a top priority for DHS, Secretary Mayorkas issued a call for action dedicated to cybersecurity in his first month in office. This call for action focused on tackling the immediate threat of ransomware and on building a more robust and diverse workforce.

In March 2021, Secretary Mayorkas outlined his broader vision and a roadmap for the Department's cybersecurity efforts in a virtual address hosted by RSA Conference, in partnership with Hampton University and the Girl Scouts of the USA [3].

The FBI is the lead federal agency for investigating cyber attacks and intrusions. It collect and share intelligence and engage with victims while working to unmask those committing malicious cyber activities, wherever they are. The FBI is the lead federal agency for investigating cyber attacks and intrusions. It collect and share intelligence and engage with victims while working to unmask those committing malicious cyber activities, wherever they are [4].

Whether through developing innovative investigative techniques, using cutting-edge analytic tools, or forging new partnerships in USA communities, the FBI continues to adapt to meet the challenges posed by the evolving cyber threat [4].

■ The FBI has specially trained cyber squads in each of our 56 field offices, working hand-in-hand with interagency task force partners.

■ The rapid-response Cyber Action Team can deploy across the country within hours to respond to major incidents.

■ With cyber assistant legal attachés in embassies across the globe, the FBI works closely with our international counterparts to seek justice for victims of malicious cyber activity.

■ The Internet Crime Complaint Center (IC3) collects reports of Internet crime from the public. Using such complaints, the IC3's Recovery Asset Team has assisted in freezing hundreds of thousands of dollars for victims of cyber crime.

■ CyWatch is the FBI's 24/7 operations center and watch floor, providing around-the-clock support to track incidents and communicate with field offices across the country [4].

Список використаних джерел:

1. About CISA – [Електронний ресурс]. – Режим доступу: <https://www.cisa.gov/cybersecurity>

2. Cyber Issues – [Електронний ресурс]. – Режим доступу: <https://www.state.gov/policy-issues/cyber-issues/>

3. Current state of Cyber Fight– [Електронний ресурс]. – Режим доступу: <https://www.dhs.gov/topic/cybersecurity>

4. FBI is the leading agency for investigating cyber attacks – [Електронний ресурс]. – Режим доступу: <https://www.fbi.gov/investigate/cyber>

Євсенкова К.,

здобувач ступеня вищої освіти магістра

Національної академії внутрішніх справ

Консультант з мови: Галдецька І.

K-9 UNIT IN THE FIGHT AGAINST ORGANIZED CRIME

Police dog is a term for a K-9, a dog that is specifically trained to assist police and other law-enforcement personnel. History has long since documented the role of the domesticated dog in human history. Its role in law enforcement has also been well documented as a helper and valuable tool in fighting crime and the criminal element. Dogs have been used in law enforcement since the Middle Ages – a tenth of the country's wealth was given to the maintenance of the parish constable's bloodhounds, who were used to hunt criminals. The rapid urbanization of London in the 19th century increased public concern regarding growing lawlessness – a problem that was far too great to be dealt with by the existing law