

*Філіппова О., студентка Університету
державної фіскальної служби України*

*Консультант з мови: Савченко А. П.,
кандидат педагогічних наук, доцент,
Університет ДФС України*

CYBER SECURITY STRATEGY OF NEW ZEALAND

New Zealand is increasingly reliant on information communication technology (ICT) and an open, trusted Internet. Internet connectivity is an integral part of New Zealand's economic growth and international competitiveness. But this technology provides opportunities for those with criminal or hostile intentions.

The 2015 Cyber Security Strategy signals the government's commitment to ensuring New Zealand is safe, resilient and prosperous online. New Zealand's scale and relatively simple telecommunications and network structure enables the public and private sector to work closely together to embed a cyber security culture, and to respond nimbly to evolving cyber risks. Four intersecting goals will create a secure, resilient and prosperous online New Zealand:

1. Cyber resilience. New Zealand's information infrastructures can resist cyber threats and we have the tools to protect our national interests;

2. Cyber capability. New Zealanders, businesses and government agencies understand cyber threats and have the capability to protect themselves;

3. Addressing cybercrime. New Zealand improves its ability to prevent, investigate and respond to cybercrime;

4. International cooperation. New Zealand protects and advances its interests on cyberspace issues internationally [1].

The main principles underpinning the Cyber Security Strategy are:

Partnerships are essential. Close partnerships with the private sector and non-government organisations are required. Businesses drive the New Zealand economy and depend on the Internet and networked technology. They must protect the information that is critical to their commercial success. The Connect Smart partnership is a public-private collaboration focused on driving cyber security improvement in New Zealand. Connect Smart includes a growing network of banks, telecommunication companies, ICT companies, software companies, social media, retail organisations, education institutions, non-government organisations, community groups, sectoral bodies, business associations and government agencies.

Economic growth is enabled. Strong cyber security practices will result in businesses remaining productive, profitable and transparent to customers and shareholders. New Zealand will be recognised as a desirable place to do business, store data, innovate and invest ICT and enhanced connectivity will continue to boost economic growth, and the costs of cyber insecurity will be minimised.

National security is upheld. Cyber threats to New Zealand - particularly state-sponsored espionage, cyber terrorism, theft of intellectual property from government and critical national infrastructure - are national security risks. Upholding New Zealand's national security in the face of this threat is a fundamental principle of this Strategy.

Human rights are protected online. The openness of the Internet is part of its unique value - allowing for unrestricted participation and the free flow of information. Cyberspace should be a trusted medium, where users have confidence in the integrity of information and the protection of their private and financial details. They should be able to engage online without suffering harm or unlawful interference. Human rights apply online as they do offline. This includes the right to freedom of expression, and the protection of privacy, as set out in New Zealand law and existing international law [2].

The Cyber Security Strategy is accompanied by a living Action Plan. This Plan will evolve to keep pace with technology developments and the emergence of new threats. New actions may be added, and existing actions amended. The National Cyber Policy Office will work with government agencies and Connect Smart public-private cyber security partners to produce a public annual report on progress.

Cyber Security Strategy Action Plan includes:

1. Cyber resilience: set up a national computer emergency response team; vigorously protect New Zealand's most important information infrastructures; use cyber tools to further New Zealand's national security interests; prepare for major cyber incidents.

2. Cyber capability: expand connect smart activities and partnership; improve the cyber security capability of small and medium enterprises; boost the cyber security capability of the corporate sector, including national infrastructure, and the public sector; promote cyber security education and training, including building a cyber security professional workforce; support cyber security research and business innovation.

3. Addressing cybercrime: build capability to address cybercrime; adapt New Zealand's policy and legislative settings for the digital age; enhance New Zealand's operational response to cybercrime; use New Zealand's international connections to fight cybercrime.

4. International cooperation: promote internet governance and norms of state behaviour that reflect New Zealand's interests; build networks of international operational cooperation; contribute to

international cyber security capability and confidence; maximise the economic opportunities of cyberspace for New Zealand and new Zealanders [1].

Список використаних джерел:

1. Ministry of Economic Development, New Zealand's Cyber Security Strategy 2015: National Plan to Address Cybercrime - December 2015, New Zealand Government at <http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-cybercrime-plan-december-2015.pdf>.
2. New Zealand Police «Prevention First: National Cybercrime Operating Strategy 2014-2017» - Wellington, 2014.