„Co-funded by the Prevention of and Fight against Crime Programme
of the European Union“

Lithuania has developed and operates a national Cybercrime Centre of Excellence

By consolidating academia and business resources a national Cybercrime Centre of Excellence for Training, Research and Education (L3CE) was established in 2013, which joined to international network of the Centres of Excellence for Cybercrime and Cybersecurity (2Centre).

The Network brings together national Cybercrime Centres of Excellence in many European Union (EU) countries and provides access to these countries' Law Enforcement Agencies (LEA) to Network resources – officers' training and certification programmes, to forensics tools, developed by researchers and scientists, to innovation and R&D results for cybercrime forensics. The network is coordinated and development of R&D is supported by few EU institutions such as EUROPOL, Joint Research Centre of the Commission, the European Cybercrime Training and Education Group (ECTEG) and others.

L3CE development was supported by the European Commission via funding the L3CE project under Prevention of and Fighting against Crime Programme for 2007-2013 (ISEC) expecting that the centre will become as competence gateway in fighting against cybercrime in Lithuania and Baltic region – Lithuanian and foreign LEA could use information, methodologies, tools, programmes etc. that will be available at the centre.

The L3CE project continues the 2Center network project idea is to establish sustainable network of Cybercrime Centres of Excellence across EU that will act as truly global collaborative platform. At fighting against cybercrime the cooperation among the EU and Lithuanian LEA and other relevant authorities is very important.

It is necessary to use the achievements of national authorities, business and academia, exchange with knowledge and best experiences, to take over achievements of other EU Member States towards the development of new curricula and new competencies. The emergence of such a centre is a timely and right step toward closer collaboration among in Lithuanian LEA and academia.

In cooperation with Lithuanian LEA – Vilnius County Police Headquarters (VCP) – 2 new curricula for Lithuanian LEA were developed during the project: the first programme – “Identity theft in Cyberspace. Legal aspects” (developed mainly by – Mykolas Romeris University) and the second programme – “Forensics investigation in a virtual environment and hidden crime information detection” (developed mainly by – Kaunas University of Technologies).

Under each programme 10 trainers were trained, who will be able to continue to train officers in the workplace, or later – through training courses. Such LEA and academia joint activity enables not only better understanding of end-users needs, but also offers the more tailored and relevant products.

The first programme devoted to LEA officials and provides knowledge about the identity and personal identification in the physical and cyber space, enabling to perceive the potential use of personal identity in cyberspace, including the illegal use of another person's identity in cyberspace.

The second programme is designed for LEA agents who carrying out criminal investigations and forensics of offences in virtual and cloud computing environments.

Other two training programmes were taken over from foreign partner – Dublin College University Centre for Cyber Security and Cybercrime Investigation (UCD), then adapted and localised in Lithuania. Such adaptation of in other EU countries developed curricula enabled to save time and resources without development of analogic programmes.

The first adapted programme – “First responders” is designed for LEA officials investigating IT use in committing the offense, but who are non-IT professionals. The programme aims to introduce training participants to the potential abuse of technology means, to provide instructions on how to effectively respond to cybercrime and to offer the methods for proper investigation of these crimes.

The second adapted programme – „Deepthought” is a training how to use forensics tool *Deepthought* and is dedicated for LEA officers who work at crime scene or search place and carry out a quick review seeking to collect only the data that has the potential to become clues, and for cybercrime forensics laboratories where very large-scale forensics are carried out. Deepthought tool reduces a number of the manual files reviews, by this increasing an efficiency of exploitation of limited resources disposing by LEA in many countries.

The latter programme become an integral part of a broader training programme – “External storage investigation”, that has been designed and tailored for LEA officers who carry out investigation of external storages possibly used for illegal use of IT to commit crime. This broader programme was developed by VCP and company Ekonominės konsultacijos ir tyrimai. Programme “External storage investigation” aims to provide training participants with the knowledge and understanding of the methods and tools for digital traces collection, to provide with information about successive stages and actions in each stage, how to prepare for and carry out digital traces collection, how to capture and record the collected evidences in order they can be recognised in judicial proceedings.

10 trainers were trained under each adapted programme and Deepthought training was emphasised a practice via using demonstration method so called on-hands training.

The project provided a great opportunity for Lithuanian LEA to access the experience of Irish colleagues during Lithuanian LEA visit to UCD (Ireland): relevant activities in the various Irish Police units were introduced and observed – in units on criminal investigations, forensics of mobile phone and video recording devices, internal surveillance systems, computer forensics, and in mobile phone forensics laboratory.

UCD also introduced a master degree programmes available to police investigators and demonstrated the developed software tools for cybercrime forensics. In showcasing the tools 3 forensic tools were selected for further adaptation and localisation in Lithuania.

The first tool – FiRST – is designed for pre-trial investigators going to crime scene or search place and carrying out analysis of live systems, especially if it is suspected that the system may contain the encryption and disk erasing software or there were some connections to cloud computing services network, turn on virtual machines, etc.

The second tool – Mighty Artefact Analyser (MAA) –is the inter-platform graphical interface-based tool for verification of the various artefacts, that found in the suspect devices, and is able quickly and accurately perform various user artefact analysis and present the results in the user-friendly form. MAA is easy to use

for any user, regardless of their expertise. The unique feature of MAA is that advanced users can create new and tailored to their needs shaped plug-ins.

The third tool – Deepthought – quickly detects graphic files, images, photos, movies, video, internet chats, e-mails, websites visited or searched, encrypted files, virtual machines according to created keyword list and generates search results report into separate evidence drive without leaving any trace on the suspect device.

Although transfer of forensic tools is the fastest way to provide with the most advanced forensic investigation tools, there is expecting in future to develop forensics tools in Lithuania too. Kaunas University of Technologies has developed on R&D results based forensics method and prototype for investigation of cybercrime in Internet of Things. Based on this method and prototype a new forensics tool may be developed later.

Experience of foreign partners was taken over in another area too: Spanish S21SEC institute, that is acting in cybercrime and cybersecurity, transferred 2 certification programmes that later were adapted and localised in Lithuania – „Electronic objects collection“ and „Windows artefacts“.

The first certification programme is dedicated to investigating officers, who work with the electronic items collection on site: officials involved in the examination of the crime scene, search, seizure and operational group of officers. The second certification programme is designed for artefact analysis of the most common operational systems – Windows – performed in forensic laboratories or police commissariats.

Lithuanian LEA officers and specialists were trained under the first certification programme and examined. The pilot training under certification programme “External storage investigation” was carried out using reality simulation method that allows not only consolidate the knowledge gained, but also to gain practical skills and avoid the mistakes.

The certificates issued to trainees, who passed an exam under training or certification programme, are attesting that officials and experts received the relevant knowledge and skills, therefore digital evidences collected by certified officers will be disputed in court more difficult. So far, this has been one of the gaps, why cyber offenders sometimes eluded punishment. In addition, more trained LEA officers and specialists will enable much faster cybercrime forensic investigation.

Developed training and certification programmes should become an integral part of national LEA competence improvement framework. It is expected that over 2,000 officials and professionals could be trained under these programme across Lithuania. Best practice on adaptation and localisation of the programmes and tools was presented at international level too. Together with suggestions on how to improve EU and EU Member States competence framework for LEA, this best practice was presented in Europol ECTEG Annual Meeting and in a round-table discussion at Germany Cybercrime Centre of Excellence that actively participating in development of national competence framework and contributes to elaboration of competence standards at EU level.

The products developed during the project are available for LEA online through L3CE web portal: there will be available to get training and certification programmes, the latest tools for cybercrime forensics, to get the R&D results and agenda of international event in cybercrime and cybersecurity topics. Over one year

operating web portal www.l3ce.eu gradually becomes not only a competence gateway for Lithuanian LEA, but also serves as an international collaboration platform for LEA in EU, EU and other countries.

Developed programmes and tools will be improved further and be shared with other Cybercrime Centres of Excellence and LEA across EU, therefore supply of means for cybercrime forensics should grow. This activity will be performed by L3CE. Prepared a long-term and medium-term strategy and operating model will contribute to a stability and sustainability of the Centre activities.

L3CE project and activity of the Centre has received recognition of the Commission in short-time: a multiplication across EU and extension of this project was funded in 2015. It is expected to strengthen collaboration among analogic EU national Cybercrime Centres of Excellence by joining them into common network where various in EU countries developed the training, certification programmes, tools, R&D results and best practices would be shared, the common standards and models will be elaborated at EU level, the joint actions will be carried out, discussions arranged and the solutions tackling to handle the new threats and problems will be offered.