© Европейската комисия

Енергетика и киберсигурност

Енергийната киберсигурност бе във фокуса на две специализирани събития, проведени в София

В А „Г. С. Раковски“, съвместно с „Платформа за образование и иновации в енергийната киберсигурност“ и със списание „Ютилитис" организира съвместно с Министерство на енергетиката обща работна среща – обучение със симулационна игра по киберсигурност за секторите енергетика и транспорт на тема: „Киберсигурността и ефектите върху енергийния и транспортния сектор на страната – готовност за реакция“. Събитието се проведе на 27 и 28 юни 2019 г. в ситуационния център на ВА „Г. С. Раковски“.

В официалното откриване на събитието приветствия към участниците отправиха генерал-майор д-р Груди Ангелов, Началник на ВА „Г. С. Раковски“, полк. проф. д-р Камен Калчев, Началник на Катедра „Комуникационни и информационни системи“ във ВА „Г. С. Раковски“, доц. д-р Атанас Георгиев – главен редактор на сп. „Ютилитис“, Димитър Стоянов – Координатор на „Платформа за образование и иновации в енергийната киберсигурност“ и Владимир Янков, ССИ на Министерство на енергетиката.

Основните акценти в обучението и в ситуационната игра по киберсигурност бяха свързани със секторите енергетика и транспорт относно готовността на екипите за реакция (ЕРИКС) на тези сектори за действие, при симулирани кибератаки, срещу инфраструктурата на енергетиката и на транспорта в страната. Обучението със ситуационна игра включи следните основни пунктове:

- Въвеждане в основната рамка на приетия в края на 2018 г. Закон за киберсигурност;
- Представяне на основните предизвикателства и заплахи пред киберсигурността на енергийните компании в сектор „Енергетика";
- Представяне на основните предизвикателства и заплахи, пред киберсигурността в сектор „Транспорт";
- Подготовка на екипите за реакция (ЕРИКС_ от двата сектора за институционалните и технически предизвикателства в сферата на киберсигурността;
- Участие на представители на екипите за реакция (ЕРИКС) от двата сектора в симулирани кибератаки, срещу определени обекти от енергийната и транспортната инфраструктура.

Лекции и презентации през участниците изнесоха:

- полк. проф. д-р Камен Калчев, Началник на Катедра „Комуникационни и информационни системи", Военна академия „Г.С.Раковски";
- представител на дирекция МИС в ДАЕУ и Националния център за действие при инциденти в информационната сигурност (CERT Bulgaria);
- Владимир Янков, Ръководител на Звено „Защита на класифицираната информация" в Министерство на енергетиката;
- Станимир Пенелов – PhD и специалист по киберсигурност ;
- Стилияна Пенева – дирекция „Информационни технологии", М-во на транспорта, информационните технологии и съобщенията;
- Детелин Йолов - системен администратор и специалист по киберсигурност в енергийния сектор, „Business Management Systems" Ltd.;
- Йордан Драганчев – търговски директор на „Техно Логика"ЕАД – София.

Семинар по киберсигурност в ядрения сектор

Основните предизвикателства пред киберсигурността в ядрената наука, енергетика и технологии бяха обсъдени на семинар по киберсигурност в ядрения сектор, организиран от Българското ядрено дружество, съвместно с платформа „Образование и иновации в енергийната киберсигурност" и Института за ядрени изследвания и ядрена енергетика (ИЯИЯЕ) на Българската академия на науките. Семинарът се проведе на 26 юни 2019 г. в ИЯИЯЕ.

Сред участниците в семинара бяха представители на ИЯИЯЕ, Държавно предприятие „Радиоактивни отпадъци", Списание „Ютилитис", Агенцията за ядрено регулиране, Държавната агенция „Национална сигурност", Посолството на Съединените американски щати в България, Индустриален клъстър „Електромобили", „АЕЦ Козлодуй-Нови мощности" ЕАД и Европейския парламент.

По време на събитието директорът на ИЯИЯЕ доц д-р Лъчезар Георгиев представи мащабния проект „Изграждане и развитие на Център за компетентност Квантова комуникация, интелигентни системи за сигурност и управление на риска (Quasar)", в който Институтът участва. В презентацията си доц. Георгиев разгледа основните цели на проекта, подходите за неговото изпълнение и важността на резултатите от него за повишаване на нивото на киберсигурност в страната и в енергийния сектор. На достъпен език той обясни основната идея на квантовия подход за криптиране на информационните потоци и предимствата, които носи за защита на процеса на пренос на информация.

В презентацията на Димитър Стоянов, координатор на платформа „Образование и иновации в енергийната киберсигурност", бе описан основният модел на взаимодействие в областта на киберсигурността в страната и взаимоотношенията между заинтересованите страни.

Интерес предизвика и презентацията на Владимир Янков, ръководител на звено „Защита на класифицираната информация" в Министерство на енергетиката. Той разгледа законовата рамка на киберсигурността в България, институционалното взаимодействие в тази област и основните заплахи, които са обект на противодействие от страна на системите за киберсигурност.