Държавни стандарти за програма „Киберсигурност“

СТАНДАРТ

■ 100 милиона са предвидени за проекти, в които ще участват университетите
■ Средствата ще се отпускат от Министерството на иновациите и растежа

Живеем във време, в което 90 процента от активностите на всеки един от нас са онлайн. Затова защитата на киберпространството отдавна не е просто една сложна парола, а цяла система, която започва с анализ на риска.

Киберсигурността вече е точка първа от защитата на националната сигурност на всяка една държава. Тя обаче изисква не просто компютърни умения, а компетентности за управление на екипи, които предотвратяват кибератаки върху огромни информационни системи, оперативно взаимодействие и вземане на решения в сложна заобикаляща среда, свързани с планиране, ръководство и управление на системи за киберсигурност в сектор сигурност. Експертизата по киберсигурност трябва да е тясно обвързана с държавната политика в сектора и с отбранителната индустрия. Затова качественото образование във висшите учебни е първата и най-важна стъпка.

Всъщност, именно връзката образование - държава - индустрия в киберсигурността е темата, която "Стандарт", съвместно с Българска академия за сигурност, поставя на фокус за поредна година. И тази година сме предвидили поредица от национални и регионални дискусии, в които ще съберем представители на изпълнителната и законодателната власт, заедно с предприятията от отбранителната индустрия и университетите, за да се дискутират създаването на държавни стандарти в обучението по киберсигурност, които да са в съответствие с целите на националната стратегия и да отговорят на нуждите от специалисти в този бранш.

100 милиона са предвидени за проекти, в които ще участват университетите

Водещ международен специалист по темата е проф. Владимир Бронфенбренер, който е председател на Българска академия за сигурност и заедно с негови колеги от Израел, държава, водещ световен фактор в областта на киберсигурността, прилагат у нас уникална методика за програма "Киберзащитници", която спаси 70 000 български деца от нараняване в нета и свали процента на застрашените у нас младежи под средния за Европейския съюз.

Националната дискусия за 2025 г. отново ще се проведе във Военна академия, която е водеща в програмата "Киберсигурност", на която като партньор сме привлекли и Софийския университет. Регионални дискусии ще се проведат до края на годината във Варна, Велико Търново, Правец и Панагюрище.

Около 100 милиона лева за проекти, свързани с киберсигурността, предвижда Министерството на иновациите и растежа. В момента се разработва методиката на финансовия инструмент и съвсем скоро той ще бъде на разположение на научните звена и бизнеса, увериха от Министерството.

8,5 трилиона долара са в световен мащаб годишните загуби в резултат на киберпрестъпления, разкри председателят на Българска академия за сигурност (БАС) проф. Владимир Бронфенбренер. Огромните загуби налагат комплексна битка с кибератаките.

Според него киберсигурността изисква знания, умения и навици, които трябва да бъдат създадени с регулацията на държавата. Индустрията е ключова, тя позволява напредване на технологиите, но първата стъпка е образованието, категоричен е експертът по сигурността.

В Израел за разлика от България има само 7 държавни университета, но от 10 години към всеки от тях има Център по киберсигурност, който се контролира от специализираната Дирекция по киберсигурност към премиера на Израел. Така експертите по киберсигурност имат стандартизирани знания и умения във всяка специалност и професия, свързана с противодействието на престъпленията в онлайн среда, добави той.

Проф. Владимир Бронфенбренер подчерта, че в Израел 8,8 млрд. долара са чуждестранните инвестиции в кибериндустрията на страната за една година. 33% от компаниите в кибериндустрията в света със стойност над 1 милиард долара са израелски, а 40% от всички недържавни инвестиции в кибериндустрията в света са в Израел. Почти 11 милиарда долара пък е експортът на продукти на кибериндустрията за 2022 г.

Изграждането на устойчива киберзащита е един от определящите елементи за изпълнение на трите основни задачи на НАТО: възпиране и отбрана, предотвратяване и управление на кризи и колективна сигурност, посочва и генерал-майор Стайко Прокопиев, началник на Военна академия "Г.С. Раковски". Той е категоричен, че академията обучава най-добрите специалисти по киберсигурност у нас. Висок процент от завършилите специалност "Киберсигурност", успешно се реализират на пазара на труда в страната, което е ясен символ за връзката на образованието с бизнеса и индустрията, казва ген.-майор Прокопиев.

Средствата ще се отпускат от Министерството на иновациите и растежа

Киберзащитата е огромна предизвикателство, подчертава главен комисар Антон Златанов, директор на Главна дирекция "Гранична полиция" в МВР. Той съобщава, че първото ниво на кибератаките е разпространението на фалшиви новини, а последното - нападенията с дронове. Първата цел на всяка терористична атака е всяването на паника. Това най-лесно става с фалшиви новини, разкрива Златанов.

Затова първата стъпка е обучението. Трябват ни тесни специалисти в борбата с кибератаките, категоричен е Златанов.

4 са големите рискове пред националната сигурност, смята Николай Николов от специализираната дирекция "Информационна сигурност", направление "Киберсигурност" в ДАНС. На първо място е прекалено лесният достъп до програми за кибератаки, които свободно се разпространяват от страни, участващи в конфликти. Тези програми са безплатни и се разпространяват направо с инструкции за употребата им.

Вторият риск е високата комплексност на кибератаките, които комбинират технологични, психологически и организационни слабости в системите за защита.

Третият риск е бързото въвеждане на нови технологии без необходимата техническа експертиза във ведомствата, които ги използват.

Използването на системи с изкуствен интелект също крие големи опасности. Човешката психика е предвидима, но когато информационните системи се обучават от изкуствен интелект, това става в пъти по-бързо, а вариациите са много и трудно предвидими.

Провеждането на форуми събиращи на една маса държава, бизнес и университети, прави опит да преодолее един от основните рискове в киберсигурността, блестящо определен от Стивън Хокинг: "Има нещо по-лошо от незнанието, това е илюзията за знание, казва Николов.

Предстои разработването на цялостна концепция за киберсигурността на България с водещо звено Министерството на отбраната, а отбранителната индустрия очаква публично-частни партньорства.

Липсата на практика в университетите е големият проблем, категоричен е Илия Марчев, управител на Милтех ЕООД. Компанията разработва оборудване и софтуер на световно ниво за бойни машини и системи. Той препоръча на университетите повече часове по практическа подготовка.

Имаме огромен проблем с кадрите. Затова образованието е изключително важно, казва и Георги Вълчанов от "Оптикс".