ИЗГРАЖДАНЕ НА МОДЕЛ НА КИБЕРСИГУРНОСТ ЗА МАЛКИТЕ И СРЕДНИТЕ ПРЕДПРИЯТИЯ

Пеньо ГЕОРГИЕВ*

BUILDING A CYBER SECURITY MODEL FOR SMES

Abstract: *This paper presents a review of literary sources in the field of cyber security modeling and management. The main objective is to help SMEs improve their level of protection against cyber attacks. The author strives to build a cyber security model that can be easily deployed in small and medium businesses.*

Key words: *cyber security, information security, corporate information systems protection, national security*

УВОД

Разглеждането на киберсигурността на малките и средните предприятия е важен момент, тъй като тяхното място е ясно поставено на *Фигура 1* и *2.* Моделът на екосистемата на киберсигурността на Европейската общност, както и моделът на националната система за киберсигурност, дефинира киберсигурността на МСП като значима част от глобалната представа. Ето защо авторът смята, че е от значение създаването на опростен модел за киберсигурност на МСП, който да бъде лесноприложим, повишавайки киберустойчивостта на националния модел за киберсигурност в рамката на стратегията за киберсигурност на ЕО.

* Авторът е главен асистент, доктор в Пловдивския университет „Паисий Хилендарски“.

Фигура 1. ***Модел на националната система за киберсигурност и устойчивост [1]***

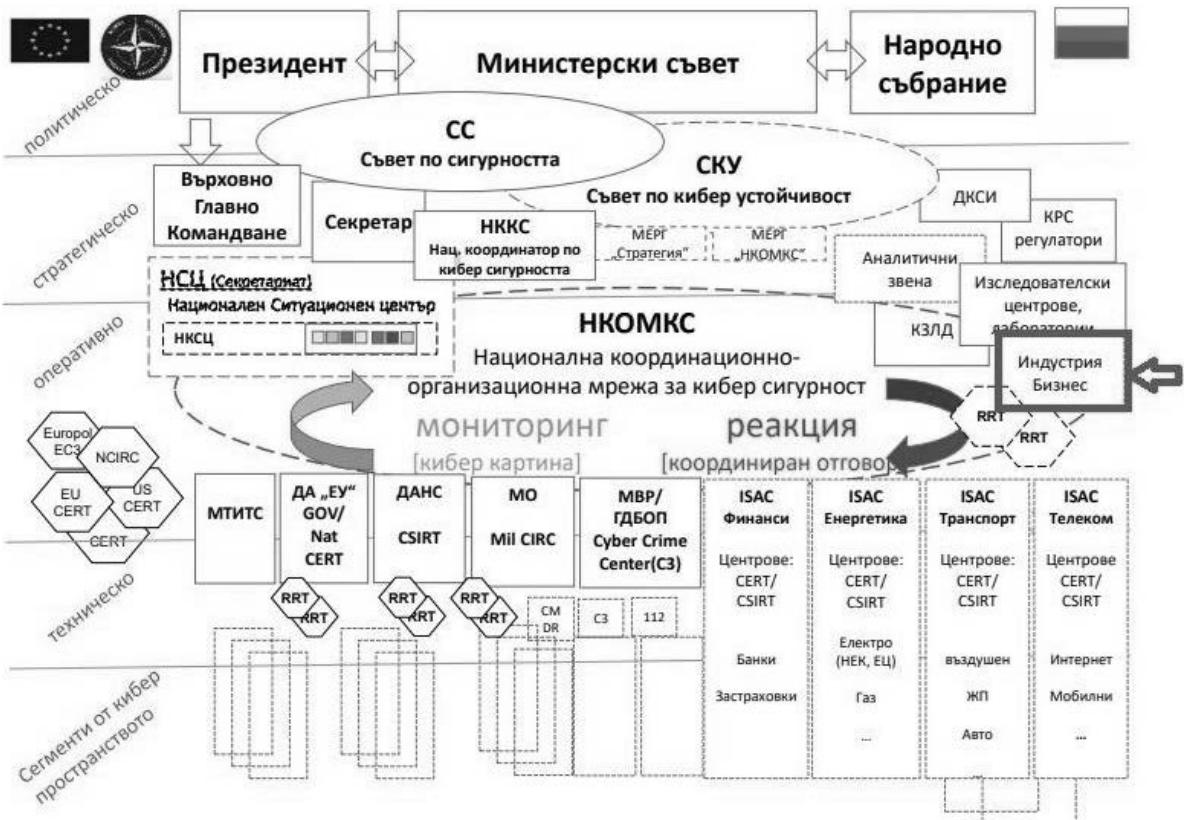


Таблица 1. **Примери за участие на заинтересованите страни в NCSS в ЕС** [5: 79 – 97]

	Area of action	Coordination of activities
Individual users	▪ Education and training. ▪ Building trust in law enforcement.	- Integration of innovation, technology and cyberspace and security teaching into school curricula (Italy) or into scientific and technical training (France). - Self-learning opportunities on cyber security website (Lithuania).
Business/private sector	▪ Public-private partnerships. ▪ Education. ▪ Investment in creating a secure cyber environment.	- Creation of consultation groups/taskforce (Netherlands) and working groups for sectorial issues (Czech Republic). - Collaboration with the public sector on processes and structures for political coordination (Austria). - Protecting SMEs through sector specific platforms in developing cyber security in relation to businesses (Austria). - Investing financial resources (UK) and other resources such as expertise, training capabilities, etc.
Critical infrastructure	▪ Building a robust critical infrastructure. ▪ Partnerships with other sectors.	- Testing critical infrastructures (Estonia). - Cross-sectorial collaboration - Information sharing within the industry (Netherlands).
CERT	▪ Collaboration with the public and private sector. ▪ Building a CERT network.	- Establishment of CERT entities in the public and private sector (Romania).
Public bodies	▪ Awareness raising campaigns. ▪ Education and training. ▪ Establish a culture of cyber security and resilience.	- Creation of training programmes and outreach activities (Lithuania). - Establishment of minimum standards of security (Austria, Czech Republic, Romania).

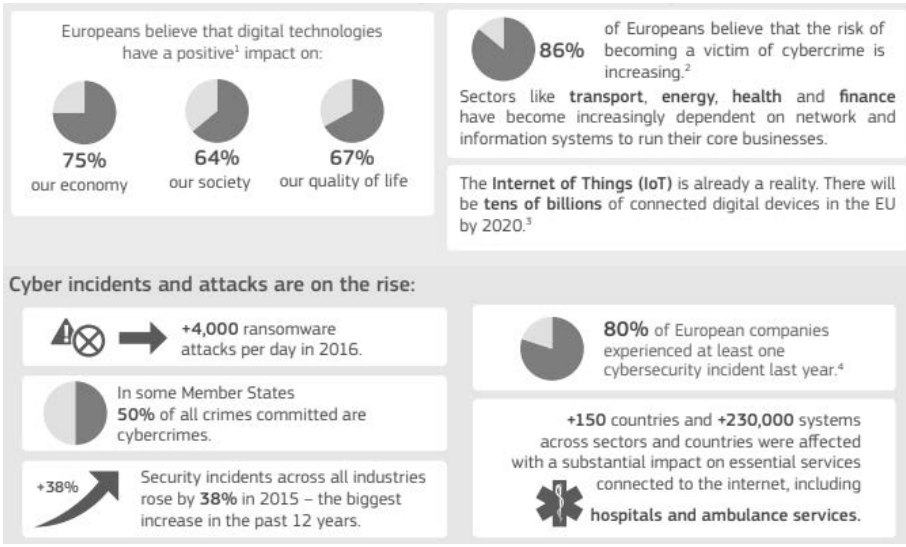
НЕОБХОДИМОСТ

Революцията в технологиите и в комуникациите коренно промени света, в който живеем. Информационните технологии промениха из основи естеството на междуличностните взаимодействия. Интернет свърза общества от всички краища на Земята. Социалните мрежи позволяват на всеки индивид да споделя информация навсякъде по земното кълбо за секунди. А глобалната мрежа ни предлага дигитално хранилище, в което всеки може да

запази срещу минимално или без никакво заплащане лична или професионална информация [5: 79 – 97].

Рисковете и заплахите в киберпространството са трудни за дефиниране поради сложността на определянето на източника на въздействие и мотивите, бързото ескалиране на заплахата, сложността и интензивността на съвременните комуникационни и информационни процеси, динамиката на логическите и физическите връзки и неопределеността на процесите [9].

Фигура 2. ***Използването на ИКТ и техните рискове за гражданите и бизнеса на ЕО***



Нарастващите киберпрестъпления и атаки са повод да се проектират стратегиите за развитие и устойчивост на киберсигурността на държавите – членки на Европейския съюз, поотделно и като обща екосистема на зоната. Според статистически данни към 2017 г. на Европейската комисия кибератаките на ден през 2016 г. са нараснали с над 4000. При 86 % от европейските граждани е изградено мнение, че рискът да станат жертва на киберпрестъпление нараства. Бизнесът все повече разчита и работи чрез информационни системи за управление, които са изцяло зависими от комуникацията през интернет. Най-малко по един инцидент, свързан с киберсигурността, е отчетен при 80 % от европейските компании през изминалата година. В някои държави членки 50 % от всички извършени престъпления са киберпрестъпления. Инцидентите в

сигурността във всички индустрии нарастват с 38 % през 2015 г. – най-много през последните 12 години.

Липсата на обучение и яснота за проблемната област е видима от фигурата по-долу. Авторът предвижда в бъдещите си разработки създаването и на модел за неформално обучение по проблемите на киберсигурността. От богатия си предишен опит с неформално обучение на мениджъри, както и с разработването на концептуален модел за неформално обучение на специалисти във винарската индустрия [6: 36 – 47], авторът ще насочи усилия към адаптиране на разработваните концепции в контекста на киберсигурността.

Фигура 3. ***Информираност и знания***

ЛОГИЧЕСКИ МОДЕЛ

В литературата се срещат задълбочено разработвани модели за киберсигурност и методи за моделиране [3, 7]. Тези модели в известен смисъл надвишават нивото на знанията на собствениците на малки и средни предприятия. Разбирането и адаптирането на такива модели предполага експертни познания и високо ниво на знания в сферата на киберсигурността, които липсват в различни сектори на бизнеса. Именно затова авторът търси решение чрез опростяване на моделите и практически насоки в помощ на МСП. Прилагането на съвкупност от разгледаните по-горе модели [6: 36 – 47, 7], както и търсенето на добри практики за бизнес организациите [2: 14 – 33] неминуемо ще доведе до повишаване на нивото киберустойчивостта в МСП. Представата за първоначална визия на модел може да се приеме от [1: 446 – 458], където са описани нивата на развитие на кибератака.

Фигура 4. ***Етапи на развитие на кибератака***

Фигура 5. ***Модел на управление на киберсигурността***

Разгледаният модел за управление на киберсигурността [8: 559 – 573] би бил подходящ за прилагане в адаптиран вариант и при МСП.

ЗАКЛЮЧЕНИЕ

Гореизложеното дава мотивация за работа върху моделирането и извеждането на полезен опростен модел за киберсигурност, насочен практически за лесно внедряване в МСП. Авторът смята бъдещите разработки да развиват концепцията за модел, отговарящ на визията на националната стратегия за киберсигурност, като същевременно са в полза и на МСП.

Литература

1. **Василев,** В. Добри практики и модели за информационната сигурност в бизнес организациите. – В: *Годишен* алманах „Научни изследвания на докторанти“, Tsenov Publishing House, 2017, с. 446 – 458.
2. **Гюров,** Р. Модел за изграждане на система за киберсигурност. – В: *Научна* конференция на тема „Защитата на личните данни в контекста на информационната сигурност“, НВУ „В. Левски“, факултет „Артилерия, ПВО и КИС“, Комисия за защита на личните данни, Държавна комисия по сигурността на информацията, катедра „Информационна сигурност“, Шумен, 2013, с. 14 – 33.
3. **Калчев,** К. Измерване на параметри в системите за киберсигурност. 2018. ISBN 978-619-7478-04-4.
4. **Национална** стратегия за киберсигурност „Киберустойчива България 2020“.
5. **Савов,** И. Един поглед върху неприкосновеността и защитата на личните данни в дигиталната ера. – В: *Бюлетин* на Факултет „Полиция“, Академия на МВР, бр. 37, 2017, с. 79 – 97. ISSN 1312-6679.
6. **Савов,** И. Един поглед върху същността на киберпрестъплението. – В: *Политика* и сигурност, ВУСИ, 2017, с. 36 – 47. ISSN 2535-0358.
7. **Angelova,** M., P. Georgiev, G. Dimitrova, D. Pastarmadzhieva. Business-Science-Education: a Collaboration for Competitive and Sustainable Growth of the Wine Industry. – In: *8th* International Scientific Conference „TechSys 2019“ – Engineering, Technologies and Systems, Technical University of Sofia, Plovdiv Branch, 16-18 May 2019.
8. **Limba,** T., T. Plėta, K. Agafonov, M. Damkus. Cyber security management model for critical infrastructure. – In: *Entrepreneurship* and Sustainability Issues, 4 (4), pp. 559 – 573.
9. *https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies*