ОБУЧЕНИЕ НА БЪЛГАРСКИ СПЕЦИАЛИСТИ С ВИСШЕ ОБРАЗОВАНИЕ ПО ИНФОРМАЦИОННА БЕЗОПАСНОСТ

Доц. д-р Агоп Саркисян
СА „Д. А. Ценов" – Свищов

Резюме: Статията разглежда въпросите, свързани с подготовката на специалисти с висше образование в областта на безопасността на компютърните технологии. Направен е анализ на възможностите за такова обучение у нас и неговите различни форми. Посочени са различните проблеми, които се срещат при такова обучение. В края на работата се прави заключението, че практически е по-уместно да се прави такова обучение като магистърска степен, т.е. като надстройка на бакалавърска степен, свързана с компютърни технологии.

Ключови думи: информационна безопасност, университетско обучение, системи за информационна сигурност, киберсигурност, анти-спам сигурност.

JEL: I20, I29, F52, D83.

TRAINING HIGHER EDUCATED BULGARIAN SPECIALISTS IN INFORMATION SECURITY

Assoc. Prof. Agop Sarkisyan, Ph.D.
„D. A. Tsenov" Academy of Economics – Svishtov

Abstract: The article is dedicated to the matters related to the preparation of professionals with higher education degrees in the field of the computer technologies security. An analysis is made of the possibilities for such an education in Bulgaria and its different forms. Outlined are the problems which could be met in such training. In the end of the work a conclusion is made, that practically it is better to organize such an education as a master degree, t. e. as a superstructure on the Bachelor degree connected to the computer technologies.

Key words: information security, university training, information ceurity systems, cyber-security, anti-spam security.

Развитието на информационните и комуникационните технологии коренно промени ежедневния живот, превръщайки се в доминиращ фактор за устойчивото развитие на обществото през XXI век. При това проблемите на информационната безопасност (или сигурност) придобиха принципно значение не само за обществото и държавата, но и за личността (отделният индивид). В по-голяма част от страните в света информационната безопасност се разглежда като съставна част от националната безопасност, която наред с енергийната, продоволствената и др. изисква осигуряване на безопасност за производствено-техническите и социално-икономическите системи, създавани от обществото. Често се използва и сходното понятие ИТ сигурност[1], което се разви значително с глобализацията на информационните услуги и появата на все по-усъвършенствано информационно общество. Така например постепенно се премина от сигурност, резултат от внедряване на един продукт, или сигурност на периметър, до интегриран подход, включващ процеси за планиране, оценка, изграждане и управление на обезопасени мрежови инфраструктури и всеобхватни програми за сигурност. Компаниите се опитват да интегрират системи за сигурност в ИТ инфраструктурата, като преоценяват архитектурите, внедряват правилни политики, обезопасяват всички нива на технологиите и намаляват оперативните си разходи, като осъществяват аутсорсинг на управлението на защитата на инфраструктурата си. С особена сила въпросите за информационната сигурност звучат понастящем в условията на т.нар. „грид компютинг" или ставащите все по-актуални напоследък облачни изчисления.

*

През 2007 г. общите разходи за софтуер за ИТ сигурност в Централна и Източна Европа достигат 344 млн. долара. IDC очаква пазарът на софтуерни продукти за информационна безопасност в региона да нарасне до средногодишен ръст от 17,8% за периода до 2012.

За да се постигнат тези мерки и да се реализират необходимите нива на безопасност на информацията, циркулираща в информационните системи от различен тип, които се използват в почти всяка човешка дейност, повсеместно все повече се чувства нуждата от кадри с висока квалификация, които да реализират ефективно необходимото обезопасяване на технологиите. Във връзка с това се отделя повишено внимание на кадровото осигуряване на информационната безопасност, на подготовката на специалисти в тази област, включително и с висша квалификация, на основата на непрекъснато усъвършенстване на образователния процес, защото теорията и практиката в областта на информационните ресурси се развиват непрекъснато, интензивно и динамично.

Анализът на учебните програми и публикациите в тази както научна, така и твърде практическа област показва, че са оформени две основни направления: в подготовката на кадри за нея: академично висше образование и специализирани курсове на различни други образователни структури, включително и екипи за обучаване във водещи ИТ-компании. Учебните планове на специалности в университетите от тип информационна безопасност предполагат изучаване на разнообразни фундаментални и по-тясно свързани с тематиката дисциплини, запознаване с текущите научно-технически достижения и формиране на специалисти с добра

[1] По въпроса за уточняване на понятието за информационна безопасност има различни схващания, но достатъчно подробен анализ бе направен например в: „**Охрименко, С. А, Саркисян, А.** Подготовка на магистри по новата специалност „Информационна безопасност", Юбилейна международна научна конференция „Информационно осигуряване на бизнеса" 7-8 юни 2006 г., Сборник, АИ „Ценов", стр. 49-57.

теоретична база и практически умения. Второто направление е свързано с осигуряване получаването на достатъчни за текущата практика знания, тяхното усъвършенстване и непрекъснато актуализиране с цел постигане на съответствие с изискванията за нивото на развитие на информационните технологии и съответстващите стандарти. Тези две направления не са в противоречие едно с друго, по-скоро се допълват, защото едното предполага дългосрочна подготовка за получаване на образователно-квалификационна степен, а второто обикновено е по-краткосрочно интензивно и конкретно обучение с много практика. Понастоящем има стремеж за съчетаването им във времето така, че веднъж придобитата фундаментална подготовка по-нататък да позволява допълване в конкретна проблематика в някои от многобройните аспекти на информационната безопасност.

Кадрите в областта на ИТ сигурността, които се подготвят в развитите индустриални страни, са с предимно с математико-технически уклон, тъй като повечето от методите за осигуряване на такава информационна безопасност са математически и програмни. Това обаче не означава, че в тази област не са необходими още и допълнителни фундаментални знания, свързани с управление, организация, поведенчески науки и т.н. Формирането на такива специалисти очевидно е задача на университетите, тъй като са необходими както професионални знания в конкретна предметна област, така и специализиращи дисциплини по информационна безопасност. Това е така, защото информацията в различните преметни области е задача на специалисти от тези области, но пък опазването ѝ от посегателства и злоупотреби изисква специални знания, свързани с осигуряването на сигурността им. Например едни форми и методи биха се използвали в областта на счетоводството и финансите, други в мениджмънта, трети в застраховането и социалното дело. Но при всички случаи е очевидно, че трябва да се интегрират както технологични, управленски, а също така и икономически знания.

Според **Michael E. Whitman,** и **Herbert J. Mattord**[2] учебният план на обучение, свързано с информационната сигурност, може да се изгражда, като се използват следните подходи:

- добавяне на елементи, свързани със сигурността към съществуващи курсове. Това е предпочитан подход и може да се използва съвместно и с другите подходи. По-добре е темите и елементите от плана, свързани с информационната сигурност, да са разпределени по цялото съдържание, а не да се добавят като отделен модул в края на обучението. Така може да се допълнят дисциплини от специалността „Информатика" или „Бизнес информатика" – например по програмиране (може да се разглеждат криптографски методи) или компютърни мрежи (вмъкват се теми за защита на мрежите), бази данни (създаване на сигурни методи за управление на данните) или системен анализ и проектиране (проектиране на информационно безопасни системи);
- елементи, добавени към обобщаващи или основни дисциплини. Например може да се въведе такова съдържание в планирането, дизайна на информационни системи или информационния мениджмънт. Вариант на подобен подход може да включва и обучението, така и курсови работи – с индивидуален или с екипен характер.
- специални, отделни дисциплини, посветени на информационната сигурност – най-често използваният подход понастоящем. В учебните планове на много специалности, свързани с компютърни технологии, се въвеждат една или две дисциплини, обхващащи проблемите на информационната сигурност. Разбира се, това

[2] Вж. **Whitman, Michael E.** Ph.D., CISSP, Herbert J. Mattord, CISSP - A (Draft) Model Curriculum for Programs of Study in Information Security and Assurance, KSU Center for Information Security Education & Awareness, Kennesaw State University, 1000 Chastain Rd. MS 1101, Kennesaw, GA 30114, USA, pp. 7.

изисква добро обмисляне на съдържанието им – видовете теми, отделните обособени части на всяка тема, хорариумът и т.н. Освен това важна е и практическата насоченост – чрез твърде много фундаментална теория (математика, теоретична криптография и т.н.) едва ли ще може да се подготви добър професионалист в областта на информационната сигурност. Балансът между теорията и практиката в тази област е особено важен.

- специализации по информационна сигурност. Те обикновено съдържат свързан набор от дисциплини, обединени по темата на информационната сигурност, при чието завършване се издава сертификат. Такава специализация изисква добро проучване на нуждите, детайлно планиране на базата на желаните резултати от завършването на програмата за специализацията.
- специалности с получаване на образователно-квалификационна степен. Много професионалисти, изследователи и експерти в областта на информационната сигурност считат, че крайната цел на една разширена и задълбочена подготовка на кадри на базата на учебен план е бакалавърската програма по такава специалност. Това обаче изисква значителни усилия да се създаде и запълни с необходимите дисциплини такава специалност на бакалвърско ниво и даже повече ресурси, за да се предложи и да привлече студенти. По-лесно е да се създаде учебен план за магистърска програма по информационна сигурност, защото магистратурата по принцип има за цел задълбочаване на знанията и по-тясна специализация в дадена област. Затова и много висши учебни заведения, които предлагат подготовка на кадри, свързани с компютърни технологии, използват този подход като по-гъвкав и по-лек за реализиране на специалисти със степени по информационна сигурност.

Когато се въвежда тематиката за информационната сигурност в обучението на студентите, може би трябва да се започне с първите два подхода и постепенно да се достигне, при наличие на необходимите ресурси (преподаватели, време, технологии, студентски предпочитания и др.), до специалност, която да дава образователно-квалификационна степен.

Специалистът по информационна сигурност с образователно-квалификационна степен (бакалавърска или магистърска) трябва да има:

- добро математическо образование, с акцент върху онези дялове от математиката, които са приложими за проектиране и разработка на системи за защита на информацията, софтуерни системи за осигуряване на информационна сигурност;
- да е достатъчно правно образован, да познава стандартите в тази област и техните изисквания;
- познания за организацията на такива системи за информационна сигурност, които включват: политиката – съвкупност от формални правила, регламентиращи механизмите за информационна безопасност; идентификацията и аутентификацията – определяне на всеки участник в информационното взаимодействие и осигуряване на увереност в това, че участникът в процеса на обмен на информация е правилно идентифициран; одита и мониторинга – проследяване на събитията, случващи се в процеса на обмен на информация (одитът предполага анализ на събитията постфактум, а мониторингът се реализира в режим на реално време); управление на рисковете – осигуряване съответствие на възможните загуби от нарушаване на информационната безопасност и др.
- формиран съвременен подход към информационната безопасност като системна научно-практическа дейност, носеща приложен характер;
- да притежава теоретична подготовка, свързана с основите на управлението на информационните системи, а също така и с информационната сигурност;

- да е запознат с основните съвременни методи и средства за защита на информацията;
- да е запознат с разпространените програмни средства и продукти и услуги за осигуряване на информационна сигурност.

Разбира се, този списък може да се детайлизира и продължи, но трябва съответният учебен план, изискванията за хорариума, т.е. времевата рамка на такава подготовка да бъде съобразена с учебно-методическите изисквания и норми, човешките и технологични ресурси. В нашата страна всички бакалавърски програми според Закона за висшето образование са с продължителност четири години и обучението по коя да е специалност трябва да осигурява получаването на 240 кредита (съгласно въведената кредитна система във висшето образование у нас). Това означава приблизително около 40 дисциплини за покриване на бакалавърска степен по дадена специалност. Очевидно 8-10 дисциплини могат да бъдат фундаментални за дадената предметна конкретна област (инженерни науки, икономика, естествени науки и т.н.), но следващите, които специализират академическото образование в областта на информационната сигурност, по наше мнение по-трудно могат да запълнят останалия хорариум. Затова в чист вид бакалавърски програми в България точно и само по информационна сигурност малко университети у нас предлагат, но има комбинирани специалности. Например Националният военен университет „В. Левски", във факултета по артилерия ПВО и КИС в гр. Шумен, предлага бакалавърска програма по „Административна и информационна сигурност".[3] Има и изключения, например Специализираното висше училище по библиотечни и информационни технологии в гр. София предлага бакалавърска програма по информационна сигурност, в учебния план на която са залегнали както фундаментални, така и специализирани дисциплини: изучават се линейна алгебра и аналитична геометрия, математически анализ, системен анализ, информационен мениджмънт, основи на компютърните системи, теоретични основи на информатиката, програмиране, информационни системи, компютърни мрежи и комуникации, методологични основи на информационната сигурност, криптография и криптология, защита на информацията в компютрите и мрежите, информационна сигурност в Интернет, защита на класифицирана информация, защита на интелектуалната собственост, нормативно-правни основи на информационната сигурност, риск мениджмънт, бизнес психология. Засега са минали три години от 4 годишната акредитирана програма. Съществуват и бакалавърски програми в българските университети, в които се четат дисциплини, в които се третират доста подробно въпросите на информационната сигурност, но носят по-общи названия. Например такава програма съществува в Софийския университет „Св. Климент Охридски" с название „Европеистика", а в дисциплината по нея „Информационно общество" се вижда, че основната тематика е свързана най-вече с въпросите за защита на информацията, личните данни, компютърната сигурност и т.н.[4] Дисциплини, третиращи въпросите на информационната сигурност, се преподават и в други бакалавърски специалности в университетите, например в университета „Св. Св Кирил и Методий" в гр. Велико Търново в специалност „Компютърни науки" се чете курс по „Компютърна сигурност". В специалностите „Информатика" и „Информатика и математика" няма такава дисциплина, но се четат дисциплини като криптология, защита на данните и др.

[3] За подробности виж URL: http://www.pv-ma.bg/priem/students.html.
[4] За подробности виж URL: http://www.eustudies.eu/show.php?storyid=692405.

**

Малко по-различно стоят въпросите с магистърските програми по „Информационна сигурност". Както вече се каза, поради по-малката времева рамка и по-различната цел на обучението – задълбочаване на знанията в по-конкретна област – магистърските програми са от 1.5 до 2.5 години и броят на дисциплините е значително по-малък. По отношение съдържанието на такава програма има различни схващания. Може би в най-обобщен вид то трябва да съдържа следното: [5]

Нормално в посочените по-горе времеви рамки би могло да се направи учебен план за магистърска програма, която да съдържа дисциплини, свързани с тероризма, хакерството, сигурността, възстановяване от бедствия, Web 2.0 технологии, правни норми, стандарти, одит, администриране на бази данни, създаване на обезопасени програми с Java, C++ и т.н. В българските университети магистърските програми по информационна сигурност също не са много разпространени в чист вид, но има различни магистратури, които по-тясно или по-широко обхващат въпросите на сигурността в информационните системи. Например в цитирания по-горе най-голям наш университет „Св. Климент Охридски" в гр. София се предлага магистърска програма „Защита на информацията в компютърните системи и мрежи"[6], която е двусеместриална, като в първия семестър се преподават 7 дисциплини – компютърни мрежи, стандарти и нормативни документи за оценка на сигурността в информационните системи, управление на информационната сигурност, компютърната сигурност, въведение в криптографията и сигурността на данни, теми за злонамерен софтуер и практикум на CISCO 2 Academy. Вторият семестър съдържа 9 дисциплини: информационна защита, системи за откриване и предотвратяване на проникванията, моделиране на защитени взаимодействия в компютърни системи и мрежова и системна администрация. Тук също има няколко практикума на CISCO академия. Програмата завършва с дипломна разработка и нейната защита.

Понякога се предлагат съвместни магистърски програми между две висши учебни заведения. Като пример за такава програма може да се посочи тази, която е резултат от разработката на Академията на МВР у нас и Специализираното висше училище по библиотекознание и информационни технологии (СВУБИТ) – програма за национална сигурност, международна политика и информационна сигурност. В тази програма се изучават дисциплини, свързани с политика, публична власт, международно и европейско право, информационен мениджмънт и административно право и процес, защита на информацията в компютрите и мрежите, информационна сигурност в Интернет, стандарти на НАТО за информационна сигурност, информационна война и информационни операции. Всичко това е събрано в два семестъра и завършва със защита на магистърска теза. Подобна съвместна програма, третираща и въпроси на информационната сигурност, се предлага и от университета „Св. Св. Кирил и Методий" – Велико Търново и Държавната комисия по сигурността на информацията в България, от СУ „Св. Климент Охридски" и др. под названието „Информационни технологии в съдебната и изпълнителната власт".

Интерес представлява и предложението за създаване на такава програма в магистърското обучение на специалност „Бизнес информатика" в цитирания вече

[5] Dan Morrill (Program Director CityU of Seattle) http://it.toolbox.com/blogs/managing-infosec/teaching-information-security-23707.

[6] За подробности виж URL: http://portal.uni-sofia.bg/docs/fmi/Zasht%20Infor% 2008.ppt #360,1.

МАГИСТЪРСКА ПРОГРАМА ЗАЩИТА НА ИНФОРМАЦИЯТА В КОМПЮТЪРНИТЕ СИСТЕМИ И МРЕЖИ.

доклад на проф. Охрименко и доц. А. Саркисян. Там според нас с достатъчно силна аргументация е посочена голяма част от аспектите, на които трябва да се обърне внимание при разработката и предлагането на такава програма по Информационна безопасност като изисквания, съдържание, организация на подготовката на методически материали и др.[7]

От посочените примери се вижда, че дори и когато става дума за ограничен по обхват учебен план, също има различни виждания за това, каква да бъде неговата структура, какъв баланс да има между теорията и практиката.

С цел постигане интензификация на подготовката на кадри с висше образование в областта на информационната сигурност, университетите в нашата страна предлагат т.нар. допълнителни квалификации, по които се издава сертификат от съответния университет. Това позволява да се проведе специализация в по-компактен вариант и при всички случаи да се запази необходимият академизъм в обучението, защото в такова обучение все пак участват преподаватели от акредитирани в това направление образователни институции. В този смисъл подобна форма е конкурентна на предлаганите множество курсове за сертифициране по информационна сигурност от различни бюра и фирми срещу заплащане. Вярно е, че последните са значително по-практически насочени, но обхватът им е доста стеснен и най-често задоволява нуждите на определен вид организации или компании.

Като примери в това отношение можем да посочим двете допълнителни квалификации, които се предлагат: а) в СУ „Св. Климент Охридски" – допълнителна квалификация по кибер сигурност и б) допълнителната квалификация към Центъра за квалификация на ВТУ „Св.Св. Кирил и Методий" по специалност „Информационна сигурност".

В първия случай специализацията е оформена като модул за квалификация с продължителност една година с два семестъра с по три дисциплини във всеки семестър и общ хорариум от 180 учебни часа. През първия семестър се изучават дисциплините: управление на кибер-сигурността, управление на антиспам сигурността и управление на анти-хакер сигурността, а през втория семестър дисциплините са ориентирани към управление на сигурността на клиентите, сървърите и JAVA приложенията. Вижда се, че е налице наистина тясна специализация в тесен конкретен обхват (компютърна и мрежова сигурност) със силна практическа насоченост, т.е. забелязва се сходството на тази програма с сертификационните курсове, предоставяни от фирми и други видове структури извън ВУЗ занимаващи се с обучение.

Във втория случай допълнителната квалификация дори се нарича специалност „Информационна сигурност" и също има модулно обучение, състоящо се от два модула с хорариум от 120 учебни часа, като в първия се изучават дисциплини по защита на данните, компютърната сигурност, защитата на информацията в Интернет, а във втория модул вниманието е насочено към сигурността в комуникациите, електронния бизнес, електронните разплащания. В тази допълнителна квалификация могат да се обучават лица със средно, бакалавърско и магистърско образование, което също силно приближава целевите групи на обучаеми, към които се насочват фирмените и други организации, предлагащи сертификационни курсове. Освен това и в двата случая се забелязва, че обхватът на разглежданата тематика е строго ограничен до конкретна предметна област.

И двете допълнителни квалификации, независимо как се наричат, завършват с издаване на свидетелство или сертификат за професионална квалификация.

[7] Вж. **Охрименко, С. А, Саркисян, А.** Подготовка на магистри по новата специалност „Информационна безопасност", Юбилейна международна научна конференция „Информационно осигуряване на бизнеса" 7-8 юни 2006 г., Сборник, АИ „Ценов", стр. 49-57.

*
* *

От направения кратък анализ на видовете обучение, които се предлагат в у нас в областта на информационната сигурност, се вижда, че определено тематиката е актуална и търсена, получаваните квалификации и степени са необходими и оценявани на различни нива – както на микроикономическо ниво в компаниите, фирмите и финансовите институции, така и в държавните и общински учреждения, а има кадри с по-голяма квалификация и съответстваща специализация, които са необходими и на национално ниво.

На второ място прави впечатление разнообразието на формите на обучение, което означава, че пазар за такива кадри има и той се развива, защото проблемите на информационната сигурност стават все повече с повсеместната електронизация на всички човешки дейности. Освен това разнообразието и различният обхват на обучение означава, че са необходими и кадри с различна квалификация съгласно нуждите на различните структури и организации в обществото.

Считаме, че в цитираното мнение на **Michael E. Whitman,** и **Herbert J. Mattord** в началото на тази работа има резон. Вероятно обаче що се касае до нашата българска практика, кадрите, които се и ще се подготвят в областта на информационната сигурност, е по-целесъобразно да се подготвят в магистърската степен поне две причини – възможност за постигане на по-голяма задълбоченост в проблематиката поради по-тесния обхват и времевата рамка и второ – поради това, че е по-гъвкаво, по-лесно и по-ефективно да се направи такова обучение като надстройка над бакалавърската степен, получена в области като компютърни науки, приложни аспекти на информатиката, математика и др.

Мениджърите по информационна сигурност и ИТ директорите в предприятията трябва да бъдат наясно с това, че предизвикателствата, които досега водеха до впечатляващ ръст на технологии за ИТ сигурност, няма да бъдат същите при сегашното забавяне на икономическия ръст и кризата в икономиката. Независимо от това обаче те трябва да съумеят да поддържат високи нива на информационна сигурност въпреки същите или дори намалени бюджети. Това има и пряка връзка с подготовката и използването на квалифициран персонал според нуждите на съответната организация, за което са предназначени и различните форми на обучение и квалификация. Все пак обаче обучението в акредитирани образователни институции в много случаи е за предпочитане пред такова обучение от различни бюра или фирми, защото получената квалификация често пъти води до много специфични области на приложение в конкретна фирма или организация.

Цитирана литература и интернет източници

1. Демирев, В. В. Безопасность информационных технологий. Системный подход. - К.: ООО ТИД Диа Софт, 2004. - 992 с.

2. Компьютерная преступность и информационная безопасность.- Мн.: АРИЛ, 2000.

3. Охрименко, С. А., Саркисян, А. Подготовка на магистри по новата специалност „Информационна безопасност”, Юбилейна международна научна конференция „Информационно осигуряване на бизнеса” 7-8 юни 2006 г. ,Сборник, АИ „Ценов” , стр. 49-57.

4. Радев, Е., Охрименко, С., Черней, Г. Информационното противостоене – възможности и оценка на риска. // Автоматика и информатика, 2000, N 2-3.

5. Саркисян, А., Охрименко, С., Черней, Г. Информационно противопоставяне. http://www.security.ase.md/publ/ru/pubru46.html

6. Тужаров Х. Д. Архитектура на информационната сигурност. Асеневци, 2010 г.

7. Черней, Г. А., Охрименко, С. А., Ляху, Ф. С. Безопасность автоматизированных информационных систем. Кишинев: Ruxanda, 1996.

8. Computing Curricula 2001. December 15, 2001. http://www.sigcse.org/cc2001

9. Dan Morrill (Program Director CityU of Seattle) http://it.toolbox.com/blogs/managing-infosec/teaching-information-security-23707

10. IT Baseline Protection Manual. http://www.bsi.bund.de/gshb/english/menue.htm

11. ISO/IEC FDIS 27001. Information technology-Security techniques-Information security management systems-Requirements. 2005-05-14.

12. Michael, E. Whitman, Ph.D., CISSP, Mattord, Herbert J. CISSP KSU Center for Information Security Education & Awareness: A (Draft) Model Curriculum for Programs of Study in Information Security and Assurance, Kennesaw State University, 1000 Chastain Rd. MS 1101, Kennesaw, GA 30114.

13. URL: http://www.eustudies.eu/show.php?storyid=692405

14. URL: http://portal.uni-sofia.bg/docs/fmi/Zasht%20Infor%2008. ppt #360,1 - МАГИСТЪРСКА ПРОГРАМА ЗАЩИТА НА ИНФОРМАЦИЯТА В КОМПЮТЪРНИТЕ СИСТЕМИ И МРЕЖИ