РЕЦЕНЗИЯ
от проф. д.ик.н. Маргарита Кирова Бонева
за научната дейност
на гл. ас. д-р ХРИСТО АТАНАСОВ ХРИСТОВ -
кандидат за заемане на научната длъжност „доцент”, в Област на висшето образование: 9. Сигурност и отбрана, професионално направление 9.1. Национална сигурност (Системи за сигурност) за нуждите на катедра „Управление на системи за сигурност“ от Факултета по технически науки на Шуменския университет “Епископ Константин Преславски”, публикуван в „Държавен вестник” бр. 26/07.04.2015г.

Единственият кандидат за заемане на академичната длъжност „доцент” има богат административен, организаторски и педагогически опит, което личи от представеното CV.

Служител е от службите за сигурност във ВКР /Военно контра разузнаване/, НСС /Национална служба за сигурност/ и ДАНС /Държавна агенция национална сигурност/. Работил е в Държавна Агенция „Национална Сигурност” в структурите на ТДНС –Варна и ТДНС Шумен. Служител е на ДАНС „Регионална Служба Сигурност ВП и ВКР”- Варна. Офицер е от ВКР. Участвал е в „Операция на ЕС – „Алтея” по укрепване на сигурността в Босна и Херцеговина” във връзка с осигуряване мисията на Българския национален контингент в операцията на ЕС –„Алтея”. Работил е с класифицирана информация на НАТО и ЕС на база издадени разрешения за достъп до КИ – „NATO SECRET” и „SECRET UE/EU SECRET”, копия на които са приложени към автобиографията. Той е контраразузнавач и оперативен работник. Заемал е длъжности от оперативен работник до Началник на сектор. Служител е на ДАНС. Ръководил е организирането на оперативната работа по линия на криминална и икономическа престъпност в гарнизоните в Шумен, Търговище, Разград, Русе и Силистра. Офицер е от БА. Бил е командир на батарея в ракетни войски на БА. Армейско звание – подполковник.

Преподавателската си работа в Шуменския университет „Епископ Константин Преславски” започва през 2012 г. като хоноруван асистент в катедра „Управление на системите за сигурност” във ФТН. От 2013 г. е главен

асистент. Чете лекции по дисциплините: Защита на класифицираната информация; Отбранителна сигурност и операции по поддържане на мира; Мениджмънт на системите за сигурност; Бъдещи кризи и конфликти и води упражнения по дисциплините: Регионална сигурност; ЗКИ; МОС; ОСОПМ; Глобализация; Конфликтология; Теоретични основи на националната сигурност; Кризи и конфликти; Глобализация и сигурност; Основи на охранителната дейност; Мониторинг на сектора за сигурност; Обществен ред и сигурност.

ОНС „доктор по организация и управление извън сферата на материалното производство – (национална сигурност) е получил във Висше Военно Артилерийско училище „Г.Димитров" –Шумен

Висшето му образование е машинен инженер, специалност „Технология на машиностроенето". Завършил е и специалност „Финансов менижмънт" в Стопанска Академия –„Димитър Ценов" –Свищов.

Владее английски и немски език. Има много добра компютърна грамотност.

Научните му интереси са в областта на националната сигурност, фирмената сигурност и стеганографията.

В обявения конкурс гл. ас. д-р Христо Христов участва с 1 монография, 3 учебника и учебни помагала, 13 -научно-теоретични статии, 24 - доклада на научни сесии и конференции и 12 съвместни доклади със студенти. Има 16 цитирания.

Представената монография «**Сигурност на фирмата и противодействие на посегателствата срещу нея**" е с обем от 328 страници, включващи увод, 6 глави, свързани с ползването и творческа обработка на 307 литературни източника (повече от една трета, от който от чужди автори). В първа глава са разгледани сигурността на социалните системи (организации) и базовите детерминанти. Втора глава е посветена на същността, структурата и задачите на системата фирмена сигурност. В трета глава е направен анализ на противодействието на посегателствата срещу фирмената сигурност. В четвърта глава е представена същността на управлението на противодействието срещу посегателствата на фирмената сигурност. В пета глава е предложен един възможен модел за организиране на противодействието срещу посегателства на

фирмената сигурност, а шеста глава изследва защитата на информацията на компютърните мрежи в бизнес организацията.

В монографията авторът, основавайки се на направения литературен преглед и на богатия си опит и знания, прави анализ на съществуващата практика. Представя механизми за управление на противодействието в сферата на фирмената сигурност, принципите за защита на активите на фирмата. Монографията е своеобразен модел за управление на противодействията на посегателството срещу нея. В нея авторът представя структурирано знание и методология за поведение на специалистите по фирмена сигурност, необходими за усвояване и изпълнение на служебните функции и задължения и придобиване на нова квалификация по аспектите на фирмената сигурност, на база изследване на концепцията на противодействието срещу посегателства на фирмената сигурност. Концепцията обединява и определя пътя за изграждане и реализиране на контраразузнавателния цикъл (КРЦ), с цел развитие на фирмата.

Предложеният комплексен подход при управление на противодействието може да бъде успешно приложен в сферата на фирмената сигурност с цел надеждно проактивно противодействие на съвременните глобални заплахи и посегателства и изграждане на гъвкава динамична система за сигурност, гарантираща изпълнението на мисията на социалната организация.

Разработеният модел за организация и управление на противодействието на посегателства в сферата на фирмената сигурност, касае процедурите за управление на противодействието в сферата на сигурността и принципите за защита сигурността на информацията и активите на организацията. В монографията са отразени резултатите от изследванията на автора в областта на фирмената сигурност, част от които са отразени в посочените в списъка на литературата публикации. Разработката основно изследва „фирмената сигурност”, поради което тя приоритетно е предназначена за тези, интересуващи се от въпросите на сигурността на бизнес организацията. Противодействието на посегателства и защитата на бизнес информацията са корпоративни въпроси и следва да са едни от основните проблеми на днешните бизнес лидери.

Монографията може да се използва за обучение на специалисти, чиито квалификационни характеристики изискват познаване на основните механизими за организиране на противодействието на различни посегателства срещу организациите и технологиите за тяхното разкриване и неутрализиране. Организацията на противодействието на посегателства срещу сигурността на фирмата в методологически аспект включва дейностите:

- създаване на система за управление на фирмена сигурност;
- задълбочено изучаване на социалната организация;
- дефиниране и оценка на ценностите и активите за защита на организацията;
- кои и какви ресурси трябва да се защитят;
- идентифициране на източниците на заплаха на дефинираните активи;
- защита на ценностите и активите;
- идентифициране на уязвимите места на системата за сигурност на организацията;
- оценка на въздействието, включително и последствията за организацията от реализацията на дадена заплаха в дългосрочен план (загуба на имидж, загуба на доставчици и пазари, финансови и материални загуби, фалит и др);
- оценка на незащитеността на организацията, чрез използване на количествени и качествени способи;
- анализ на съществуващите и планирани механизми, форми, методи и способи за противодействие и защита.

В учебното пособие «**Демокретичен контрол на сектора за сигурност**» се дискутират въпроси, свързани с механизмите за контрол над институциите от сектора за сигурност на Република България. Основна цел на пособието е студентите да получат знания и практически умения, за да могат успешно да прилагат изследователските подходи, методическия апарат и техническите инструменти за осъществяване на контрол над организациите от сектора за сигурност в Република България. В модулите му е охарактеризирана същността и функциите на гражданския контрол на сектора за сигурност. Посочени са начините за реализиране на граждански контрол чрез предложения и сигнали на гражданите; обжалване по административен

ред на индивидуалните и общите административни актове; оспорване на административните актове пред съда; защита срещу неоснователни действия или бездействия на администрацията на сектора за сигурност; търсене на отговорност от държавата за вреди; използване възможностите за граждански контрол на институцията на омбудсмана.

В учебното помагало «**Основи на охранителната дейност**”, с автори Н. Досев и Х. Христов**,** е направен анализ на възможностите на структурите от системата на МВР, занимаващи се с охранителна дейност, както и натрупаният в това отношение опит в държавите членки на Европейския съюз и извън него. Разгледани са проблемите, свързани със същността, организацията и правната уредба на частната охранителна дейност на територията на Република България.

Основна цел на пособието е студентите да получат начални знания и практически умения, след усвояването на които ще могат успешно да прилагат наличните изследователски подходи, методически апарат и технически инструменти за организиране и управление на реална охранителна дейност в сферата на частния бизнес.

Ръководството за упражнения по стеганография с автори С. Станев, С. Железов, Х. Параскевов и Хр. Христов е предназначено за осигуряване на практическите упражнения по дисциплината „Компютърна стеганография, изучавана от студентите от Шуменския Университет „Епископ Константин Преславски». То може да се използва с успех и при обучение по дисциплините „Компютърна и мрежова сигурност, „Защита на данните, „Информационна сигурност и други в предметната област „Информационна сигурност. В него авторите посочват, че методите на съвременната компютърна стеганология се прилагат в областта на военните и правителствени комуникации, защитата на авторското право и при решаването на задачите по осигуряване на информационната сигурност. Стеготехниките могат да се прилагат както за целите на защитата на данните, така и за незаконни цели – например, за създаване на скрити канали за изтичане на забранени документи и за комуникация на престъпници. Ново предизвикателство за специалистите в областта на стеганологията са и он-лайн социалните мрежи (ОСМ). На разработването на нови стеганометоди, алгоритми и софтуер и

усъвършенстване на вече съществуващите са посветени множество както явни, така вероятно и много секретни изследвания. Чрез Интернет на свободен режим са достъпни вече хиляди компютърни стеганографски приложения. Актуалността на тези проблеми изисква запознаването с основите на съвременната стеганология на по-широк кръг от специалисти, чиято задача е не само разработването, анализа или противодействието на стеганосредствата, но и квалифициран избор на съществуващите стеготехнологии и тяхното умело използване за решаване на конкретни приложни задачи в областта на защитата на информацията.

Учебното пособие «**Основи на охранителната дейност**» разглежда проблемите, свързани със същността, организацията и правната уредба на частната охранителна дейност на територията на Република България. Използва се от студенти на всички специалности, имащи отношение към проблемите на сигурността. Основна цел на пособието е студентите да получат начални знания и практически умения, след усвояването на които ще могат успешно да прилагат наличните изследователски подходи, методически апарат и технически инструменти за организиране и управление на реална охранителна дейност в сферата на частния бизнес.

Модулът за електронно обучение „**Организация на физическата и техническа охрана**” предлага на обучаемите студенти от специалността „Управление на системите за сигурност", обучаващи се в образователна квалификационна степен „бакалавър” знания, свързани с организацията на физическата и техническа охрана на обекти на защита, предмет на дисциплината „Основи на охранителната дейност”.

Предмет на модула е „Организацията на физическата и техническа защита”, с акцент върху същността и изискванията за разработване на основните видове вътрешнонормативни документи в стационарен обект за охрана, решаване на тестове и практически задачи за подпомагане познанията на обучаемите за изработването на алгоритъм на поведение и инструктаж за действия в различни казуси, чрез анализ на зададени ситуации.

Публикациите, с които кандидатът участва в конкурса могат да се класифицират в следните основни направления:

- Изследване и анализ на сигурността на организационно и национално равнище.
- Организиране и управление на противодействието на посегателства срещу сигурността на социалната организация.
- Стеганологична защита на информацията на социалната организация.
- Защита на личните данни на социалната организация.

В направлението „**Изследване и анализ на сигурността на организационно и национално равнище" се разглеждат** подходите за идентифициране на уязвимостите на системата за сигурност на социалната организация и компютърните ресурси; еволюцията в схващанията за сигурността; нередностите и измамите при усвояване на средствата от ЕС – заплаха за националната и фирмената сигурност; подходите за оцеляване при терористичен акт; аспектите на общата политика за сигурност и отбрана на ЕС; подходите, свързани с изследване сигурността на фирмата; кибернетичните измерения на съвременната война; трафикът на хора с цел сексуална експлоатация; аспектите на сигурността на банковите транзакции, осъществявани чрез ПОС терминал, дебитни и кредитни карти; корупцията в Р. България".

В направлението «**Организиране и управление на противодействието на посегателства срещу сигурността на социалната организация" са представени** активната и пасивната стратегии за управление на противодействието на посегателства срещу бизнес-организацията; аспектите на управлението на противодействието срещу посегателства на фирмената сигурност; модели и подходи за организиране на противодействието срещу посегателства на фирмената сигурност".

В третото направление, а именно **«Стеганологична защита на информацията на социалната организация"** се посочва, че вътрешните заплахи за социалната организация са особено трудно разрешим проблем, защото има много начини да се открадне информация от нейната мрежа, чрез използване на стеганографски методи и способи. Проблемът с тези заплахи е актуален и той официално е поставен под номер 2 в списъка на най-трудните проблеми – HPL (Hard Problem List), на Американският съвет за изследване на сигурността на информационните системи – INFOSEC. Това е списък на най-

трудните и най-критичните предизвикателства в INFOSEC изследванията, които трябва да бъдат решени за разработването и внедряването на надеждни системи за правителството на САЩ.

Обоснована е необходимостта службите за сигурност на фирмите да извършват стеганографска защита на компютърните мрежи от външни атаки и разузнаване**.** Заедно с ежедневната дейност за спиране на нежелан трафик, вируси, зловреден софтуер, и други несанкционирани опити за достъп до тях, тези служби трябва да имат предвид и вътрешни нарушители в корпорациите, които използват дигитални носители за секретно разпространяване на информация извън охранявания от мрежите периметър.

Анализирана е опасността от използването на съвременната компютърна и мрежова стеганография за създаване на канали за изтичане на секретна информация от вътрешни за дадена фирма нарушители, и предлага активна система за наблюдение от страна на фирмените служби за сигурност,за организиране на стеганографска защита на чувствителна информация и възможностите за криминални разследвания на стегоинциденти.

Изследвана е същността на въвеждане на определение за стеганологична подсистема за защита на информацията (СПСЗИ), която е определена, като част от системата за защита на информацията (СЗИ).

В четвъртото направление „**Защита на личните данни на социалната организация”** са представени статии и доклади, в които авторът изследва направлението за създаване на скрити канали за изтичане на информация, каквото е стеганографията. Посочени са класическите стеганографски методи за скриване и нерегламентирано извличане на лични данни от организацията. Разгледани са и възможностите на методите на компютърната и мрежовата стеганография-направления на информационната сигурност, изучаващи проблемите на скриване на информация в явна информационна среда, създавана от компютърните системи и мрежи. Разгледана е организацията на защитата на личните данни в социалната организация.

Посочено е, че посегателствата срещу личните данни са обективно съществуващи в действителността негативни обществени явления.

Освен това, кандидатът посочва, че динамично променящите се заплахи и произтичащите посегателства, пораждат редица проблеми, касаещи

оцеляването, гарантирането на сигурността и развитието на организациите и индивидите. В тази връзка адекватната защита на личните данни на организацията се превръща в световен проблем.

Гл. ас. д-р Христо Христо е ръководил 4 дипломанта.

Участвал е в 2 национални, 4 университетски и 2 други университетски проекти, които не са финансирани от Шуменския университет.

В преподавателската си работа д-р Христов широко прилага новите образователни технологии, проявява взискателност, прецизност и компетентност. Водените от него учебни занятия са обезпечени със съвременна и актуална литература в това число и такава, която е предложена от самия него или авторски колективи, в които той е активен участник.

Високата му ерудиция и богат практически опит са предпоставка за задълбочените и с практическо приложение проблеми, разглеждани в научната му продукция в т.ч. монография, учебни помагала, научни статии и доклади.

Умението му да работи в екип и уважението, с което се ползва сред студентите се доказва и от 12 ^{те} съвместни разработки със студенти и разработените под негово ръководство дипломни работи, свързани с актуални проблеми на сигурността.

В заключение считам, че научната продукция на гл. ас. д-р Христо Христов е свързана с актуални проблеми на националната сигурност, фирмената сигурност, стеганографията и е плод на високата му ерудиция и компетентност.

Теоретико-практическите приноси на научната продукция на кандидата са свързани със:

1. Сигурността на организационно и национално равнище.
2. Научни решения, допълващи разработени концепции, стратегии и политики, насочени към осигуряване на ефикасно социално управление, противодействие на престъпността и защита на националната сигурност, чрез засилени и усъвършенствани мерки за превенция и разкриване на нередностите и измамите при усвояване на финансови средства на ЕС.
3. Аспектите на общата политика за сигурност и отбрана на ЕС.
4. Специфичните измерения на съвременната кибернетична война.

5. Нови подходи при вземане на решение за избор на стратегия за управление на противодействието на посегателства в различни сфери (социалната организация, бизнес-организациите, фирмената сигурност).
6. Модел на стегоинциденти.
7. Система за стеганологична защита на информацията.
8. Анализ на опасностите при използване на съвременната компютърна и мрежова стеганография за създаване на канали за изтичане на секретна информация.
9. Предложени възможности за използване на класическите контраразузнавателни методи за противодействие на каналите за изтичане на конфиденциална информация.
10. Мерки за защита на фирмената сигурност.

Имайки предвид, всичко изложено по-горе убедено считам, че гл. ас. д-р Христо Христов е изграден научен работник в областта на националната сигурност и преподавател с богат професионален и практически опит, с висока ерудиция, притежаващ компетенциите за заемане на академичната длъжност „доцент”.

Ето защо, убедено препоръчвам на многоуважаваните членове на Научното жури гл. ас. д-р Христо Христов да бъде предложен на ФС на ФТН за избор за заемане на академичната длъжност „доцент” в област на висшето образование: 9. Сигурност и отбрана, професионално направление 9.1. Национална сигурност (Системи за сигурност) за нуждите на катедра „Управление на системи за сигурност“ от Факултета по технически науки на Шуменския университет “Епископ Константин Преславски”.

РЕЦЕНЗЕНТ:

(ПРОФ. Д.ИК.Н. М. БОНЕВА)