Р Е З Ю М Е Т А

на монография, учебници, статии и доклади на гл. ас. д-р Христо Атанасов Христов, представени за участие в конкурс за академична 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 Факултет Технически Науки на Шуменския университет "Епископ Константин Преславски", публикуван в „Държавен вестник" бр. 26/07.04.2015г.

1. Монография

Христов Х., Сигурност на фирмата и противодействие на посегателствата срещу нея, УИ ШУ „Епископ Константин Преславски", Шумен, 2014. ISBN 978-954-577-981-7.

Представената за рецензия монография е посветена на един актуален за нашето съвремие проблем – защитата на сигурността на фирмата, в контекста на предизвикателствата пред националната сигурност на държавата.

Сигурността на бизнес организацията очевидно се превръща в ключов фактор, един от тези, които са в състояние да и осигурят конкурентно предимство. Осъзнавайки това, ръководителите на фирми се стараят, полагат усилия и влагат ресурси в стремежа си да ги предпазят от посегателства и да организират и управляват ефективно противодействие. Повишаването на сигурността на фирмата и противодействието на опитите да се посегне на тайните и не би могло вече да се остави в ръцете на случайни и некомпетентни служители. Очевидно е назрял моментът за по-активна намеса на учени от различни клонове на науката, които биха могли по-ефективно не само да консултират, но и да структурират и непосредствено да участват в процесите на фирмената защита. В тази връзка монографията е посветена на проблем, чиято актуалност не подлежи на съмнение.

В процеса на утвърждаване като компонент на националната система за сигурност, фирмата е обект на въздействие на многообразни и сложни съвременни посегателства, като промишлен шпионаж, нелоялна конкуренция с нейните разновидности, нерегламентиран достъп до фирмената тайна, международен тероризъм, корупция и др.

Всички тези дейности са свързани с неетични и незаконни действия, които не следва да бъдат подценявани и пренебрегвани. Посочените посегателства, като деяния, са с изключително висока степен на опасност, поради косвения негативен ефект върху националното стопанство и имат негативен ефект върху резултата от извършваната дейност от бизнес организациите, а именно – тяхната печалба.

Обобщавайки изложеното по-горе, основателно може да се постави въпроса: „Подготвени и готови ли са нашите фирми за организиране на ефективно противодействие срещу професионални и сложни атаки от местни и чуждестранни сили, както и на конкурентите?".

В тази връзка монографията предлага възможен модел за управление на противодействието на посегателствата срещу фирмената сигурност, разглеждан като съвременен подход, чието приложение в сферата на сигурността позволява осъществяването на комплексно неутрализиране на многообразните и взаимозависими посегателства и надеждно предотвратяване на негативното им въздействие спрямо търговските организации.

Противодействието на посегателства срещу фирмената сигурност е разгледано като сложен процес, свързан със събиране, обработка и анализ на разнородна и голяма по обем информация. Той, като неделим елемент от системата „Фирмена сигурност", е един от основните фактори за сигурността на бизнеса. Липсата на приета нормативна база в Р. България, разглеждаща процеса на противодействие, води до това, в бизнес организациите да се прилагат разнородни модели на процеса за противодействие на заплахи и посегателства. Това налага необходимостта да се анализира съществуващата практика и да се предложи възможен, научно обоснован ефективен модел за дейностите по противодействие на заплахи и посегателства на бизнеса. Ето защо монографията осигурява запълването на един вакуум в теоретично и практическо отношение.

Като цяло стремежът на автора е да представи механизимъм за оптимизиране на процеса по управление на противодействието в сферата на фирмената сигурност, принципите за защита на активите на фирмата. Разяснени са основните средства, способи, методи и дейности за защита на фирмената сигурност, принципите и механизмите за изграждане и управление на системата за фирмена сигурност.

Проектиран е и е предложен възможен за внедряване модел на процеса по противодействие на посегателства в бизнес организациите с използване на активна стратегия, чрез която да се осигури повишаване на ефективността на процеса на противодействие, понижаване на незащитеността и вредоносните последици.

Предоставено е 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: защита на секрети, неутрализиране на заплахи, понижаване на незащитеността и предотвратяване на посегателства.

Изведени са ключови параметри и особености на видовете посегателства върху фирмената сигурност, позволяващи разработване на стратегия и модел за управление на противодействието.

Основна постановка, формулирана в разработката – управлението на противодействието е комплексен подход, който може да бъде успешно приложен в сферата на фирмената сигурност за надеждно проактивно противодействие на съвременните глобални заплахи и посегателства, за изграждане на гъвкава динамична система за сигурност, гарантираща изпълнението на мисията на социалната организация.

Със създаването на модел на процеса на противодействието в сферата на фирмената сигурност се унифицира процесът, създават се единни правила и процедури в бизнес организациите.

Разработеният модел за организация и управление на противодействието на посегателства в сферата на фирмената сигурност допринася за прилагане на адекватен на предизвикателствата проактивен подход за противодействие на видовете посегателства. Моделът касае „Процедурите за управление на противодействието в сферата на сигурността" и принципите за защита сигурността на информацията и активите на организацията.

В съдържателно отношение монографията е разработена в 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 и шеста глава изследва защитата на информацията на компютърните мрежи в бизнес организацията.

В първа глава - **Проблеми на сигурността и сигурността на фирмата в частност** е разгледана сигурността на социалните системи и са определени базовите детерминанти. Направен е анализ на литературата по темата, задълбочено са разгледани съвременните теории за сигурността на социалната организация и е поставен акцентът на социологическия и системен подход в изследването на сигурността на фирмата.

От направения анализ на публикациите по разглеждания проблем се вижда, че опитите да се теоретизира проблема за сигурността на организациите, не са от вчера. Специално внимание е отделено на теорията за сигурността, с анализ на елементите на нейния абстрактен модел, начините и средствата на нейното поддържане и защита, формите и равнищата й, както и взаимодействието между тях. Теориите за сигурността на социалните организации са представени кратко, но с необходимата пълнота и достатъчност. По-подробно са анализирани класификациите на видовете сигурност дадени от Н. Слатински, като с фигури и схеми са обяснени, същността , смисъла и съдържанието на категорията „сигурност". В заключение на прегледа на литературните източници, авторът приема работно определение за сигурността на социалната система в частност фирмата.

В глава втора - Фирмена сигурност, същност, структура, задачи е насочена към: формиране на становище за същността на понятието „система фирмена сигурност", нейните структура и функции; определяне на системата за фирмена сигурност като общо средство за противодействие на всички възможни посегателства; определяне на видовете посегателства и техните възможни форми, методи и способи за реализиране, в контекста на необходимо условие за организиране на ефективно противодействие. В главата са изследвани видовете посегателства срещу сигурността на фирмата, тяхната същност и етапи за реализиране.

Целите на глава трета - Същност на противодействието на посегателства срещу фирмената сигурност са свързани със: идентифициране на същността и смисъла на противодействието на посегателства срещу фирмената сигурност и връзката му с класическото контраразузнаване; извеждане на видовете дейност, осъществявана от звената за фирмена сигурност в противодействието на посегателства срещу фирмена сигурност; определяне на възможните специфични сили, средства, способи и методи, използвани от звената за сигурност на бизнес организацията в противодействието на посегателства срещу фирмената сигурност; формиране на становище за нормативната база, регламентираща функциите, целите, задачите и дейността на фирмените звена за сигурност, правните им възможности за ползването на средствата и методите на оперативно издирвателната дейност за защита на фирмената сигурност; изграждане на мнение относно взаимодействието между държавните и фирмените, по същество, оперативно-издирвателни служби, както и за възприемането на фирмената сигурност като елемент от защитата на националната сигурност.

Глава четвърта - **Управление на противодействието срещу посегателства на фирмената сигурност.** В главата противодействието на посегателствата и прилагането на подхода на управление на противодействието в сферата на фирмената сигурност е дефинирано и разгледано като един от възможните механизми за повишаване ефективността на процеса по защита сигурността на бизнес организациите от съвременните посегателства. В тази връзка в този раздел са разгледани целесъобразността от прилагане на подхода на управление на процеса на

противодействието и приоритетно прилагане на проактивни стратегии за управление на промените в средата за сигурност.

Глава пета - Организиране на противодействието срещу посегателства на фирмената сигурност – един възможен модел. Организацията на противодействието на посегателства срещу сигурността на фирмата е представен като изключително важен етап в процеса на управление на бизнес организацията, характеризиращ се със сложна съставна същност и включващ определени взаимно свързани дейности и процедури. Комплексното и прецизно осъществяване на всяка една от дейностите е предпоставка за постигане на висока степен на обективност на анализа и оценката на незащитеността на организацията и създаване на условия за рационалност на процеса на организиране на противодействието.

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 – от какво трябва да се защитят ценностите и активите и каква е вероятността конкретната заплаха да се реализира;

– идентифициране на уязвимостите на системата за сигурност на организацията – уязвимите места, които могат да бъдат атакувани;

– оценка на въздействието, което реализирали се заплахи оказват на организацията – какви могат да бъдат последиците за организацията при реализиране на дадена заплаха(несанкциониран достъп, промишлен шпионаж, разкриване на конфиденциална информация), включително и последствия 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[1].

Комплексното разглеждане на посочените дейности е задължително условие за извършването на надеждно противодействие на посегателствата за организацията. Подценяването на някой от компонентите или непълното му характеризиране не би позволило извършването на надеждно идентифициране на посегателствата и би възпрепятствало осъществяването на последващите етапи от процеса на организация на противодействието.

Глава шеста - **Защита на информацията на компютърните мрежи в бизнес организацията.** В главата са изследвани информационната сигурност на автоматизирана информационна система на бизнес организацията и системата за стеганологична защита на информацията. Разгледан е възможен стегоканал за изтичане на конфиденциална информация на база възможностите за използване на стеганографията в социалните мрежи FACEBOOK и GOOGGLE+. Предложени са мерки на контраразузнавателно противодействие чрез изграждане на подсистема за информационна сигурност на фирмата.

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.

Авторът не претендира за изчерпателност, всеобхватност и оригиналност на изложението. Всичко това е трудно постижимо в условията на протичащите в обществото ни изключително динамични социални и законодателни промени. Стремежът е в сравнителен план да се изложат най-важните аспекти на процеса на управление на противодействието срещу посегателства на организацията, както и да се подложат на дискусия някои спорни въпроси относно защитата на фирмената сигурност.

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. Приемането на активна стратегия за противодействие на посегателства и защита на корпорацията следва да са ангажимент на нейното ръководство. Тази дейност става обичайна в сферата на собствената сигурност на фирмата. Основен неин клиент е частният бизнес.

Монографията може да се използва за обучение на специалисти, чиито квалификационни характеристики изискват изучаване на основните механизими за организиране на противодействието на различни посегателства срещу организациите и технологиите за тяхното разкриване и неутрализиране. Разработката синтезира знания за различни аспекти на сигурността на организациите, които могат да се използват от обучаемите както поотделно, така и в определени комбинации в зависимост от специалността във висшите учебни заведения.

В тази връзка тя може да се използва с успех при обучение на студенти по специалностите „Системи за сигурност", „Корпоративна сигурност", „Административна сигурност", „Организационна сигурност" и „Информационна сигурност".

Трудът притежава и необходимите качества за използването му като пособие за самоподготовка, за придобиване на необходимата квалификация за заемане и изпълнение на ръководни длъжности, изпълняващи функции, свързани със сигурността на организациите.

2. Пособия

2.1. Христов Х., Демократичен контрол на сектора за сигурност, УИ ШУ "Е.К.Преславски" , Шумен, 2015. ISBN 978-619-201-026-3.

В условията на световна криза на международната сигурност все по-осъзната и актуална се явява необходимостта от осъществяване на ефективен контрол над организациите от сектора за сигурност на отделната държава. Прилагането на тези основополагащи принципи в практиката на публичния мениджмънт се постига посредством оптимизиране на управленската отговорност в посока осъществяване на адекватен и ефективен вътрешен, парламентарен, обществен и граждански контрол над организациите за сигурност.

В тази връзка в настоящото учебно пособие 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.

Учебното пособие „Демократичен контрол на сектора за сигурност" е предназначено основно за студентите от специалност „Системи за сигурност" с образователно-квалификационна степен „Бакалавър", с професионално направление „Национална сигурност" и

област на висшето образование „Сигурност и отбрана“, както и за обучаеми от други специалности по професионално направление „Национална сигурност“.

Пособието „Демократичен контрол на сектора за сигурност“ се вписва в обучението на посочените специалисти, като изгражда фундамент на базата на знания в основните направления, определящи контрола на организациите от сектора за сигурност на държавата. В учебното съдържание са включени няколко модули.

В ***глава първа*** на пособието е формулиран секторът за сигурност на държавата. Посочени са функциите на специализираните организации: Национална служба за охрана; ДА „Национална сигурност”; Национална разузнавателна служба; ДА „Технически операции”; ДА „Държавен резерв и военновременни запаси”; ИА „Електронни съобщителни мрежи и информационни системи“.

В ***глава втора*** са разгледани подходите за изясняване същността на категорията „контрол”, контролът като обществено отношение и контролът като функция на управлението. Направена е характеристика на контрола в направленията обект, предмет и функции на контрола.

Анализирани са видовете контрол: държавен, обществен и граждански контрол; общ и специализиран контрол; външен и вътрешен контрол; парламентарен, административен, съдебен и прокурорски контрол; данъчен, финансов, банков, митнически и застрахователен контрол; одит; мониторинг.

Посочени са формите и методите на контрол. Основни форми: предварителен, текущ, последващ контрол. Конкретни форми: наблюдение; проверка; ревизия; контролна диагностика.

Методи за контрол. Общи методи: факторен и количествен анализ; синтез; прогнозиране. Специфични методи: обследване; проучване; разследване; експертна оценка (експертиза); моделиране.

В ***глава трета*** са формирани способите за получаване на информация за контрол: отчетност; сведения; справка; анкета; интервю; фотоснимка; инвентаризация; документална проверка; писмени обяснения; разпит; претърсване и обиск.

Структурирани са органите и технологиите за контрол. Специални контролни органи: Сметна палата; Агенция за държавна финансова инспекция; Национална агенция по приходите; Агенция „Митници”.

В ***глава четвърта*** е анализиран вътрешният контрол в организациите от сектора за сигурност. Структури и функции за вътрешен контрол в Министерството на отбраната и в Министерството на вътрешните работи. Структури и функции за вътрешен контрол в ДА „Национална сигурност”, в Национална разузнавателна служба и в ДА „Технически операции”.

В тази глава са разгледани и: Парламентарният контрол на сектора за сигурност; Формиране на стратегията и на политиката за национална сигурност; Парламентарните механизми за контрол; Същността на парламентарните дебати, парламентарни питания, парламентарни анкети и разследвания, слушане в комисиите; Парламентарен контрол на разузнавателните (контраразузнавателните) организации.

В главата е дефиниран и обществеият контрол на сектора за сигурност, неговата същност и характеристики. Разяснен е контролът, осъществяван от: политическите партии; неправителствените организации; от профсъюзите; от средствата за масово осведомяване.

Охарактеризирана е 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.

Предложената структура на пособието осигурява възможност за самостоятелна подготовка на обучаемите, чрез изложените сравнително къси единици учебен материал за идентифициране, описване, дискутиране и сравняване на същностните въпроси и синтезиране на подходи за обезпечаване на контрола и мониторинга на сектора за сигурност.

2.2. Досев Н., Христов Х., Основи на охранителната дейност, УИ ШУ "Е.К.Преславски" , Шумен, 2015. ISBN 978-619-201-025-6.

През последните години на дневен ред бяха поставени и проблемите, свързани с гарантирането на личната сигурност на отделния индивид, опазването на живота, здравето и имуществото на гражданите в контекста на личните права и свободи, гарантирани от Конституцията на Република България.

Анализът 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, показват, че за ефективна защита на членовете на обществото и активите на многобройните промишлени и административни обекти освен силите на МВР е необходимо привличането и на частни охранителни дружества, отговарящи на изискванията на Закона за частната охранителна дейност.

Настоящото учебно пособие е посветено на проблемите, свързани със същността, организацията и правната уредба на частната охранителна дейност на територията на Република България.

Учебното пособие „Основи на охранителната дейност" е предназначено основно за студентите от специалност „Системи за сигурност" на ШУ „Еп. К. Преславски" в професионално направление „Национална сигурност", но би могло успешно да се използва и от студенти и от други 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.

Пособието „Основи на охранителната дейност" се вписва в обучението на посочените специалисти чрез изграждането на фундаментална база от знания в областта на частната охранителна дейност. В учебното съдържание на пособието са включени пет глави, проследяващи възникването, развитието и съдържанието на частната охранителна дейност.

В ***глава първа*** на учебното пособие са разгледани възникването, същността и развитието на частната охранителна дейност. Посочени са целите, принципите, задачите, видовете дейности и изискванията към частната охранителната дейност.

В глава втора е анализиран процесът за лицензиране и контрол на частната охранителна дейност в Република България, както и механизмите за взаимодействие между частните охранители с органите на МВР.

В ***глава трета*** са формулирани правата и задълженията на лицата, извършващи частна охранителна дейност. Предложен е вариант на методика за извършване на охранително обследване на обекти, подлежащи на физическа и техническа охрана.

В ***глава четвърта*** е направен преглед на задачите, изпълнявани от частните охранителни дружества при извършване на различните видове дейности, регламентирани от Закона за частната охранителна дейност.

В ***глава пета*** са предложени варианти на примерни документи за частните охранителни дружества, извършващи физическа и техническа охрана на стационарен обект, съгласно изискванията на закона и другите регламентиращи документи.

Предложената структура на пособието осигурява възможност за самостоятелна подготовка на обучаемите чрез изложените сравнително къси единици учебен материал за описване, дискутиране и сравняване на същностните въпроси и синтезиране на подходите за организацията на физическата и техническа охрана на обекти на защита, предмет на частната

охранителна дейност, разглеждана като един от компонентите на сектора за сигурност в Република България.

2.3. Ръководства

2.3.1. Станев, С, С. Железов, Х. Параскевов и Х. Христов. Ръководство за упражнения по стеганография. УИ "Епископ Константин Преславски", Шумен, 2015. ISBN 978-619-201-011-9.

Учебното пособие е предназначено за подготовка и провеждане на практически упражнения по дисциплините „Компютърна и мрежова сигурност“ със студенти от специалностите „Управление на системи за сигурност“ и „СОСТ“, и „Компютърна стеганография“ със студентите от специалност „Информатика“ на ШУ. То включва упражнения по симетрично и асиметрично криптиране на информация, класификация и термини на класическата и високотехнологичната стеганография, основни методи на компютърната стеганография, мрежова стеганография на базата на протокол TCP/IP, методи на стеганализа. Отделено е внимание на традиционните методи на стеганографията, използвани от службите за сигурност и на подходите и средствата за защита на информацията срещу използване на стеганографски методи от злоумишленици. Разгледана е работата с подходящ софтуер за стеганография и стеганализ.

2.4. Електронен модул за дистанционно обучение на студенти.

2.4.1. Христов Х., Организация на физическата и техническа охрана, УИ ШУ "Е.К.Преславски" , Шумен, 2014.

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".

В дисциплината "Основи на охранителната дейност" сигурността на фирмата е определена като състояние на относителната й устойчивост, постигана чрез съвкупност от дейности за превенция, разкриване и неутрализиране на различни опасности и форми на въздействие. Тези дейности, поради сложния им характер и необходимостта рационално да се комбинират и използват, не могат да се извършват само от структурите на предприятието, реализиращи стопански задачи. Поради това е необходимо да се изгради специализирана система за сигурност.

Структурата за сигурност на фирмата може да се изгради като дирекция или звено с различен състав, съответстващ на икономическия субект. Това изграждане се предшества от експертиза, която може да се извърши от назначен специалист (специалисти) или от частна консултантска агенция. Експертизата се реализира на базата на бизнес плана на фирмата. След експертизата избраният експерт (експерти), който ще консултира и контролира изграждането на дирекция "Сигурност", предлага па мениджъра проект за организационна структура, съобразен с особеностите на предприятието и бранша, както и с резултатите от експертизата.

В съответствие с тези основни постановки, се изгражда структура за сигурност на фирмата на базата на дейностите за защита на икономическия субект. За целта, групирайки опасностите и заплахите и ранжирайки ги според начина и мястото на въздействие върху фирмата, са определени следните стратегически направления в дейността на дирекцията (звеното) "Сигурност":

-външно направление (външна сигурност) - обезпечава параметрите на сигурността при взаимодействие със средата, партньорите и конкурентите;

-вътрешно направление (вътрешна сигурност) - обезпечава параметрите на сигурността при вътрешнофирмените процеси и отношения;

-физическа и техническа защита - обезпечава режима на безопасност на обектите на фирмата и на структурата за сигурност.

Предмет на разглеждане в настоящият модул е третото направение в структурата за сигурността на социалната организация а именно „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.

Обобщавайки изложеното по-горе, основателно може да се изложи съждението, че ефективна защита на ценностите и активите на охраняваните обекти от професионални и сложни атаки на външни сили, както и на конкурентите им, се постига чрез задължително използване на възможностите на охранителната дейност.

Ето защо проблематиката, свързана с охранителна дейност е изключително актуална и значима. Нейното познаване осигурява ефективна организация на защитата на ценностите на всяка организация срещу посегателства, което ще осигури: установяване на общи процедури и шаблонни документи за процеса по управление на защитата на обектите за охрана; разработване на оптимизиран модел за организиране на процеса на охрана от посегателства срещу фирмата.

3. Статии и доклади от научни конференции, сборници и периодични издания

Публикациите 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.

3.1. Изследване и анализ на сигурността на организационно и национално равнище.

1.2.25.Христов, Х., Боянов, П., Трифонов, Т. Доклад на тема: „Подходи за идентифициране на уязвимостите на системата за сигурност на социалната организация и компютърните ресурси", Journal scientific and applied research vol 5, 2014, p.101-108;

1.2.26.Krastev, K. and Hristov, H., „Development of war fare and counter-terrorism", Кръстев, К. и Христов, Х., Доклад на тема: „Развитие на военното дело и борбата с тероризма", Journal scientific and applied research vol 6, 2014;

1.2.29. Кръстев, К. и Христов, Х., Доклад на тема: „Еволюция в схващанията за сигурността", Научна конференция „Новата парадигма за сигурност в киберпространството", НВУ „В. Левски" , Факултет „Артилерия, ПВО и КИС", 5-6.06.2014 г.

1.2.31. Марков, Ю., Христов, Х., „Нередностите и измамите при усвояване на средствата от ЕС – заплаха за националната и фирмената сигурност", Трета международна научна конференция –„Наука, образование, иновации", посветена на 145 годишнината на БАН и 35 годишнината от космическия полет на Георги Иванов, 21-23.05.2014 г., Шумен.

1.2.33. Досев, Н Христов, Х., Доклад на тема: „Неправителственият сектор и националната сигурност", Трета международна научна конференция –„Наука, образование, иновации", посветена на 145 годишнината на БАН и 35 годишнината от космическия полет на Георги Иванов, 21-23.05.2014 г., Шумен.

1.2.34. Христов, Х., Стоянов, В, Доклад на тема: „Аспекти на сигурността на банковите транзакции, осъществявани чрез ПОС терминал, дебитни и кредитни карти", Научна конференция „Новата парадигма за сигурност в киберпространството", НВУ „В. Левски" , Факултет „Артилерия, ПВО и КИС", 5-6.06.2014 г.

1.2.41. Христов, Х., Доклад на тема: „Подходи за оцеляване при терористичен акт", Научна конференция „MATTEX 2014", проведена в ШУ „Еп. Константин Преславски" на 22-22.11.2014 г., докладът е публикуван в сборник научни трудове;

1.2.42. Христов, Х., Доклад на тема: „Аспекти на общата политика за сигурност и отбрана на ЕС", Научна конференция „MATTEX 2014", проведена в ШУ „Еп. Константин Преславски" на 22-22.11.2014 г., докладът е публикуван в сборник научни трудове;

1.2.44. Христов, Х., Доклад на тема: „ПОДХОДИ СВЪРЗАНИ С ИЗСЛЕДВАНЕ СИГУРНОСТТА НА ОРГАНИЗАЦИЯТА - ФИРМАТА", Годишник на Техническия факултет на ШУ „Еп. Константин Преславски", 2014;

1.2.46. Hristov, H., Доклад на тема: „Forms, methods and contrivances to materialize encroachments on business organization", Journal Science education innovation, vol. 4, 2015.

1.2.47. Христов, Х., и Тодоров, Н., Доклад на тема: „Теоретични подходи относно проблематиката на сигурността", В: Сборник трудове на научна конференция „Научна сесия 2013", Факултет „Артилерия, ПВО и КИС" на НВУ, Шумен, 2013;

1.2.48. Христов, Х., и Чобанов, М., Доклад на тема: „Аспекти на сигурността на бизнес организацията", В: Сборник трудове на научна конференция „Научна сесия 2013", Факултет „Артилерия, ПВО и КИС" на НВУ, Шумен, 2013;

1.2.49. Илиев, Св. и Христов, Х., Доклад на тема: „Заглушаване на взривни устройства", Институт по отбрана – Конференция „Military Technologies and Systems (MT&S 2013)", София, 02-03.12.2013 г.

1.2.55. Стаменова, А., и Христов, Х., „Кибернетичните измерения на съвременната война", изнесен и приет за публикуване в „Научна сесия 2014", НВУ „В. Левски" , Факултет „Артилерия, ПВО и КИС", 23-24.10.2014 г.;

1.2.56. Василева, Р., и Христов, Х., „Организирана престъпност. Трафик на хора с цел сексуална експлоатация". изнесен и приет за публикуване в „Научна сесия 2014", НВУ „В. Левски" , Факултет „Артилерия, ПВО и КИС", 23-24.10.2014 г.;

1.2.57. Казакова, И., и Христов, Х., „Защита от домашно насилие", изнесен и приет за публикуване в „Научна сесия 2014", НВУ „В. Левски" , Факултет „Артилерия, ПВО и КИС", 23-24.10.2014 г.

1.2.58. Маринова, П., и Христов, Х., Доклад на тема: „Диплома без стойност – Корупция в образователната система на Р.България", Научна конференция „MATTEX 2014", проведена в ШУ „Еп. Константин Преславски" на 22-22.11.2014 г., докладът е публикуван в сборник научни трудове.

Докладите са посветени на заплахите за сигурността на организацията и на държавата.

1.2.25. В доклада „Подходи за идентифициране на уязвимостите на системата за сигурност на социалната организация и компютърните ресурси" е защитена тезата, че идентифицирането и оценката на уязвимостта е процес, чрез който се оценяват „слабостите на системата за физическа сигурност, персонална сигурност, процедурите или други области на функциониране на организацията, които могат да бъдат експлоатирани. Предназначението на процеса е да се разкрият слабости в системата за

сигурност, информационните системи и мрежи и незащитената ключова инфраструктура на организацията“.

Уязвимостта е дефинирана като недостатък или слабост на системата за сигурност на дадена социална организация, която може да бъде умишлено или инцидентно експлоатирана и, в резултат от това, да се получат нарушения на политиката за сигурност на организацията.

Недостатъците или слабостите могат да се отнасят към цялостната архитектура или към проектираните и прилагани механизми и процедури за защита и контрол на системата за сигурност. Всяка социална организация изгражда своя собствена система от механизми и процедури за сигурност, в съответствие със законови и административни разпоредби и стандарти в сферата на сигурността и средата на функциониране на организацията.

1.2.26. Докладът „Развитие на военното дело и борбата с тероризма“ разглежда тероризмът като един от основните фактори водещи до исторически изменения в международната среда за сигурност, кореспондиращи с развитие на военното дело и до съответни промени във въоръжените сили, в това число и на армията. Изследвано е развитието на тероризма и са определени неговите актуални характеристики като всеобхватност, многоаспектност и настъпателност, които налагат адекватен отговор на обществената система за сигурност. Доколкото тероризмът използва бойни похвати и средства за постигане на своите цели и задачи, дотолкова е необходим и военен отговор на неговите предизвикателства. Подобен отговор е основно прерогатив на вътрешните органи за сигурност, които наред с армията реализират инструментариума на военното дело. Независимо от този факт, развитието на военното дело предоставя на армейските структури оперативни способности за успешно противодействие на асиметричните заплахи на тероризма. Това предполага усъвършенстване на бойната дейност чрез нови подходи при решаване на основни въпроси, характеризиращи функционирането на армейските структури.

Те предполагат създаване на: нови структурни и функционални модели на специализирани войскови подразделения със съответното окомплектоване, въоръжение и обучение; компетентни командни звена; осигуряване на взаимодействие с други национални ведомства и международни армейски формирования.

1.2.29. Новите реалности в света и в Европа, натрупаният от страната ни международен авторитет и последователната й принципна политика на добросъседство и сътрудничество са важна предпоставка за успешното отстояване на националните интереси и сигурност. Съществуващите днес рискове и заплахи за националната сигурност изискват съвършено нов тип подход, образование и обучение на служителите от институциите, ангажирани и отговорни за гарантирането на националната сигурност и мир в страната, адекватни на променената стратегическа среда и новите мисии. Настъпващите промени налагат разработването и актуализирането на концепцията за национална сигурност, военната доктрина и национална военна стратегия на Република България. Те ще наложат промени в отделните доктрини за използването на войските и силите на оперативно и тактическо ниво.

В тази връзка в доклада „Еволюция в схващането за сигурността“ са анализирани няколко определения на понятието сигурност дадени от изтъкнати експерти в областта на националната и международна сигурност. Охарактеризирани са нивата на сигурността и класификациите на сигурността. Посочено и анализирано е определението за национална сигурност заложено в устава на ООН.

1.2.31. В доклада „Нередностите и измамите при усвояване на средствата от ЕС – заплаха за националната и фирмената сигурност”, са изследвани възгледите, идеите,

концепциите, стратегиите и инструментите за превенция и противодействие на измамите и нередностите по фондове, инструменти и програми съфинансирани от ЕС и от НБ на Р България. Предложени са варианти на научни решения допълващи разработените концепции, стратегии и политики, насочени към осигуряване на ефикасно социално управление, противодействие на престъпността и защита на националната сигурност, чрез засилени и усъвършенствани мерките за превенция и разкриване на нередностите и измамите. Приложението им поражда множество научно приложни проблеми и задачи, решаването, на които е предизвикателство за научната общност у нас и в ЕС като цяло.

1.2.33. В доклада **„**Неправителственият сектор и националната сигурност“ се обобщава ролята и значението на неправителствения сектор в процесите на генерирането и защитата на националната сигурност. На първо място неправителствения сектор създава прозрачност в процесите по намиране на решения в сферата на сигурността, като наблюдава и осъществява контрол върху процеса на вземането на решения й извършват мониторинг на действията на правителството и другите субекти участващи в осъществяването на политиката за сигурност. На второ място, сектора изготвя и предоставя независими експертизи, които улесняват вземащите решения в работата им, предоставят алтернативни решения и концепции за разрешаване на актуални проблеми на сигурността, с което допринасят за провеждането на по-ефективна политика в сферата на сигурността. Трето, гарантира информираността и просветата на обществото по политическите процеси на вземане на решения, събужда съзнанието на гражданите за определени глобални проблеми в сферата на сигурността и повишава представителността на хората на националната и международната сцена.

1.2.34. Съвременното развитие на икономическия живот, се характеризира с висока степен на интензивна глобализация, повишена необходимост от конкурентноспособност и ограниченост на такива субективни ресурси като разполагаемо време. Един от методите за пестене на труд и време е въвеждането на безкасовото плащане. В тази връзка докладът „Аспекти на сигурността на банковите транзакции, осъществявани чрез ПОС терминал, дебитни и кредитни карти“ е насочен към изследване на сигурността на извършваните финансови операции, като този въпрос е разгледан в два аспекта, защита на устройствата и защита на банковите карти. Предложени са конкретни мерки за защита на осъществяваните транзакции.

1.2.41. През последните години тероризмът се проявява като една от основните опасности за сигурността на отделните държави, региони и за международната сигурност като цяло. Заплахата от тероризмът днес има много измерения. Страховата психоза, както и чувството за нестабилност, които тероризмът поражда сред обществеността, неизбежно упражняват влияние върху политическите, социалните и икономическите решения в национален, регионален и глобален мащаб.

Световната и вътрешната значимост на разглеждания проблем аргументират необходимостта от провеждане на обучение на обществеността в разпознаване на специфичните рискове и заплахи, действия и реагиране при кризисни ситуации. В тази контекст в доклада „Подходи за оцеляване при терористичен акт“ са систематизирани и анализирани конкретни подходи за оцеляване при терористичен акт.

1.2.42. Докладът „Аспекти на общата политика за сигурност и отбрана на ЕС”. Общата политика за сигурност и отбрана е най-бързо развиващата се политика на Европейския съюз. Европейският съюз се превърна в ключов партньор при разрешаване на конфликти и управление на кризи. Силата на ЕС е в използването на различни инструменти в сферата на сигурността, не само военни, но и политически, икономически и социални. ОПСО заменя предшестващата я европейска политика за сигурност и отбрана (ЕПСО). Договорът от Лисабон въвежда промяна в наименованието на

политиката и тя се обособява в нов раздел на Учредителните договори на Европейския съюз. По този начин Договорът от Лисабон подчертава важността и специфичните особености на ОПСО, която е неразделна част от общата външна политика и политика на сигурност. Въвежда и нови клаузи, целящи развитието на ОПСО. Основните нововъведения целят поетапното изграждане на обща европейска отбрана. ОПСО осигурява на ЕС оперативен капацитет, който се базира на граждански и военни средства, до които Съюзът може да прибегне при изпълнение на мисии извън територията на Съюза, с цел да осигури поддържането на мира, предотвратяването на конфликти и укрепването на международната сигурност, в съответствие с принципите на Устава на ООН /Чл. 28 А/. Държавите-членки предоставят на разположение на ЕС граждански и военни способности, за да допринесат за реализиране на определените от Съвета цели в областта на ОПСО. Ангажиментите и сътрудничеството в областта на ОПСО са съвместими с ангажиментите, поети в рамките на НАТО, която остава за държавите-които членуват в нея, основа на колективната им отбрана и главна инстанция за нейното осъществяване. Целта е чрез една по-изявена роля на ЕС в областта на сигурността и отбраната да се допринесе за жизнеността на един обновен Атлантически съюз в съответствие с договореностите от т. нар. „пакет Берлин +”.

1.2.44. В доклада „ПОДХОДИ СВЪРЗАНИ С ИЗСЛЕДВАНЕ СИГУРНОСТТА НА ОРГАНИЗАЦИЯТА - ФИРМАТА”са представени няколко възможни подхода и разбирания за обединяване на широките теоретични възгледи и перспективи, относно проблематиката на сигурността на организациите. Прието е, че сигурност за една социална система (човек, организация, общност, общество, държава, общност от държави) има тогава, когато основните идеали, ценности, потребности и интереси на системата не са подложени на никакви въздействия (абсолютна безопасност) или незастрашени от съществуващи въздействия, които социалната система да не е в състояние ефективно да неутрализира (защитена безопасност), контролира (относителна сигурност) или управлява (трансформационна сигурност).

Посочено, е че за гарантиране на сигурността истинското мениджърско предизвикателство е да се намери онова, изискващо възможно най-малък преразход на ресурси, състояние на устойчивост, в което бизнес организацията намира оптималния си баланс между несигурност и безопасност.

1.2.46. В доклада „Forms, methods and contrivances to materialize encroachments on business organization” е посочено, че видовете посегателства срещу сигурността на социалните организации са изключително разнообразни и затова, нерядко подценявани от мениджърите. Анализирани са етапи за реализация на всяко посегателство, които са: формиране на намерение, събиране на информация, анализ на информацията, изготвяне на план, осигуряване на необходимите ресурси, предприемане на действия. За всеки етап са характеризирани признаците, които могат да бъдат доловени и анализирани с цел прилагане на превантивни или защитни мерки.

1.2.47. В доклада „Теоретични подходи относно проблематиката на сигурността”е прието разбирането, че проблематиката на сигурността изисква познаване и прилагане както на дескриптивни, така и на теоретични подходи. В направено изследване са представени няколко „възможни подхода за обединяване на широките теоретични възгледи и перспективи, относно проблематиката на сигурността.

Дескриптивният подход на анализ предполага интегриране на картината на обстановката (ситуацията) и на възможните алтернативи на решения от различни документи, данни, факти, изследвания на обществено или експертно мнение и т.н. и поради това, той се реализира предимно чрез емпирични или индуктивни методи (извличане на теория от фактите).

Теоретичния подход, в същия контекст, се свързва с използване на компютърни модели и симулации или обикновени логико-математически методи на дедукция (т.е. на прогнозиране сбъдването на събития на основата на теория). На тази база се генерират изводи и се извличат тенденции.

Стратегическият подход представлява анализ и оценка на ситуациите и заплахите, прогнозиране, синтез на концептуален модел, изработка на варианти на целенасочени поведения (решения) и подпомагане избора на най-подходящ измежду тях.

Системният подход се основава на принципите на общата теория на системите и динамиката им и е свързан със системния анализ и синтез. Прилагането му се регламентира от разбирането, че проблематиката на сигурността обхваща: социална система – тази на междуфирмените отношения; специфична за всяка организация социална система; сложни социални процеси.

1.2.48. Докладът „Аспекти на сигурността на бизнес организацията" разглежда многоаспектността и класификациите на сигурността. За най всеобхватно изследване на многоаспектността е прието това на Георги Стефанов за който: „Понятието „сигурност" има много широк обем и е многоаспектно. Така е, защото проблемът дали сигурността е налице, дали липсва или е недостатъчна, възниква всякога и навсякъде, където се съчетават условията: състояние, представляващо ценност за субекта; неопределеност на бъдещето; връзка между тези два елемента, при която бъдещето на състоянието зависи от неопределеното развитие" .

Съчетаването на условията е необходимо, защото липсата на което и да е изключва възникването на проблеми, свързани със сигурността. Ако състоянието не представлява ценност, никой не би се загрижил за неговото постигане или запазване. Ако бъдещето е определено категорично и еднозначно, независимо от това дали то носи сигурност или отнема сигурност, проблеми също не възникват.

1.2.49. Поради широко разпространената достъпност до евтини електрически вериги и радиочестотни технологии значителна част от самоделните взривни устройства са радио-контролируеми детонират се дистанционно чрез някаква радио-комуникационна връзка. В тази връзка в докладът „Заглушаване на взривни устройства" е изследвана и представена за ефективна възможна форма за заглушаване на импровизирани радиоконтрилируеми взривни устройства чрез комуникационно регулиране. Заглушаването чрез комуникационно реагиране, от друга страна е обещаваща технология за този тип приложения, тъй като в сравнение с по-ограничените от гледна точка на параметрични качества заглушители използвани до момента, те извършват широколентов анализ на радио спектъра или т.нар. преглеждащи фази и са способни да реагират на потенциални заплашителни сигнали. По време на последвалите след това заглушителни фази цялата налична предавателна енергия може да се фокусира само върху съответните спектрални зони в които се намират потенциалните заплахи, което води до значително подобряване на ефективността на заглушаване или разширяване на защитния радиус.

1.2.55. В доклада **„**Кибернетичните измерения на съвременната война", са разгледани измеренията на новата евентуална битка между цивилизациите. Кибервойната не са хакерски атаки и друг вид информационен вандализъм, посочено е, че истинската кибервойна е пропаганда, изолация, изнудване и демотивация на врага. Google, Skype, Facebook, GMail и т.н. са големият световен "Биг Брадър". Супер-компютрите на тези организации вероятно са повече и по-мощни от тези в класацията по-горе. Тези социални мрежи са оплели паяжината си около почти всеки човек на Планетата, те знаят кой какво пише, какъв e-mail изпраща, какви сайтове посещава, какви пароли за банковите си сметки ползва. Невроните мрежи с лекота ще засекат

всеки потенциален екстремист според писанията му по форуми или посещенията му в сайтове.

1.2.56. В доклада „Организирана престъпност. Трафик на хора с цел сексуална експлоатация“ е анализирано Европейското разбиране за „организирана престъпност"-престъпност, в която съучастници са криминални групи, политически и други лица, а извлечените от престъпната дейност средства се използват за политически цели. Най-често организираната престъпност е дейност на управляващите, независимо от коя партия са, защото единствено те разполагат с властов държавен ресурс. Единственият мотив, от който се води този вид престъпност, е икономическият, което я лишава от творчеството и разнообразието на мотивирания от други ценности законен живот. Направена е характеристика на участниците в престъпните организации. На преден план са изведени черти като: притежаващи личностни дефицити, страхливи, трудно преодоляващи елементарните предизвикателства в живота.

1.2.57. В докладът „Защита от домашно насилие“, са изследвани същността, формите и причините за възникване на този вид престъпност. Най-общо насилието се дефинира като упражняване на действия насочени спрямо индивид или група индивиди, въпреки тяхната воля и заявено несъгласие. Разграничаването на видовете насилие има за цел да облекчи разбирането на проблема. То се проявява по различен начин, в зависимост от това кои са неговите извършители, кои са жертвите и какви са отношенията между тях. Този вид престъпление нарушава достойнството и интересите на личността.

Домашно насилие е всеки акт на физическо, сексуално, психическо, емоционално или икономическо насилие, както и опитът за такова насилие, принудителното ограничаване на личния живот, личната свобода и личните права, извършени спрямо лица, които се намират в родствена връзка, които са или са били в семейна връзка или във фактическо съпружеско съжителство.

За психическо и емоционално насилие върху дете се смята и всяко домашно насилие, извършено в негово присъствие.

В доклада са посочени и мерките за зашита от домашното насилие са: задължаване на извършителя да се въздържа от извършване на домашно насилие; отстраняване на извършителя от съвместно обитаваното жилище за срока, определен от съда; забрана на извършителя да приближава пострадалото лице, жилището, местоработата и местата за социални контакти и отдих на пострадалото лице при условия и срок, определени от съда; временно определяне местоживеенето на детето при пострадалия родител или при родителя, който не е извършил насилието, при условия и срок, определени от съда, ако това не противоречи на интересите на детето; задължаване на извършителя на насилието да посещава специализирани програми; насочване на пострадалите лица към програми за възстановяване.

1.2.58. „Диплома без стойност – Корупция в образователната система на Р.България”, Образованието представлява най-големият елемент от публичния сектор и основно човешко право, което служи като двигател на личното, социалното и икономическото развитие. Критичната заплаха за упражняване на човешките права се изразява в най-висока степен от корупционните практики. Корупцията е проблем, пред който е изправена всяка една страна, всяко едно общество и всеки един човек. Диверсионните актове, в които участва подкупничеството, отреждат българското образование в „зоната за бедствено положение". В доклада са изследвани същността и причините на корупцията в образованието, формите на проявление и са предложени мерки за противодействие. Корупцията във висшето образование не се свежда само до предлагане, искане и взимане на подкупи. Тя е всеки преднамерен начин на изпълнение на публичните дейности във висшето образование, при който се променя

качествено неговият характер, в реда-на обществения интерес и в ущърб на правата и интересите на отделните граждани. Ефектът от корупцията в образователната сфера оказва влияние върху цялата обществена система, защото висшето образование дава кадри и за бизнеса, и за държавната администрация, и за управлението. Ръководствата на висшите учебни заведения притежават достатъчно инструменти за ограничаване на корупционния обмен, достатъчно е единствено той да бъде идентифициран като проблем.

3.2. Организиране и управление на противодействието на посегателства срещу сигурността на социалната организация.

1.2.17. Христов, Х., Доклад на тема: „Активна и пасивна стратегии за управление на противодействието на посегателства срещу бизнес организацията – предимства и недостатъци", В: Сборник трудове на международна научна конференция „Младите в науката – инвестиция в бъдещето", Секция „Проблеми на сигурността", Университет по библиотекознание и информационни технологии, София, 2013;

1.2.18.Христов, Х., Доклад на тема: „Аспекти на управлението на противодействието срещу посегателства на фирмената сигурност", В: Сборник трудове на международна научна конференция „Младите в науката – инвестиция в бъдещето", Секция „Проблеми на сигурността", Университет по библиотекознание и информационни технологии, София, 2013;

1.2.19. Христов, Х., Доклад на тема: „Фирмена сигурност – характеристики", В: Сборник трудове на научна конференция „Научна сесия 2013", Факултет „Артилерия, ПВО и КИС" на НВУ, Шумен, 2013;

1.2.20. Христов, Х., Доклад на тема: „Стратегии за управление на противодействието на посегателства срещу бизнес организацията – теоретични подходи", В: Сборник научни трудове на научна конференция „Актуални проблеми на сигурността", Научно направление „Мениджмънт в сигурността и отбрана" на НВУ „В. Левски", В. Търново, 2013;

1.2.21. Hristov, H., Доклад на тема: „Aspects of the organization for counteraction to attacks against the company security"/„Аспекти на организацията на противодействието срещу посегателства на фирмената сигурнност", Journal Science education innovation, vol. 1, 2013;

1.2.23.Христов, Х., Доклад на тема: „Активната стратегия за управление на противодействието на посегателства срещу бизнес организацията – същност", Годишник на Техническия факултет на ШУ „Еп. Константин Преславски", 2013;

1.2.24.Христов, Х., Доклад на тема: „Изучаване на социалната организация – елемент от организацията на противодействието на посегателства срещу фирмената сигурност", Годишник на Техническия факултет на ШУ „Еп. Константин Преславски", 2013;

1.2.27. Hristov, H., Dimanova, D., „A model about organizing a counteraction to encroachments on company security", Христов, Х., **Диманова, Д.,** Доклад на тема: **„**Модел за организиране на противодействието срещу посегателства на фирмената сигурност". International Conference on Bionics and Prosthetics and Mechanicsq Mechatronics and Robotics, Volune 10, Latvia 2014, p. 96-105.

1.2.36. Христов, Х., „Passive strategy for management of counteraction to encroachments on business organization", Hristov, H., „Пасивна стратегия за управление на противодействието на посегателства срещу бизнес организацията", Journal scientific and applied research vol 6, 2014;

1.2.37. Hristov, H., „APPROACHES ABOUT EVALUATION ON THREATS' INFLUENCE UPON SOCIAL ORGNIZATION", Journal Science education innovation, vol. 3, 2014;

1.2.38. Hristov, H., „THE COMPANY SECURITY SYSTEM – A CONTRIVANCE TO COUNTERACT TO ALL POSSIBLE ENCROACHMENTS“ Journal Science education innovation, vol. 3, 2014;

1.2.39. Христов, Х., „Подходи за дефиниране и оценка на ценностите и активите за защита на социалната организация“, изнесен и приет за публикуване в „Научна сесия 2014“, НВУ „В. Левски“ , Факултет „Артилерия, ПВО и КИС”, 23-24.10.2014 г.;

1.2.40. Христов, Х., „Подходи за оценка и анализ на незащитеността и механизмите за защита на социалната организация“, изнесен и приет за публикуване в „Научна сесия 2014“, НВУ „В. Левски“ , Факултет „Артилерия, ПВО и КИС”, 23-24.10.2014 г.;

1.2.43. Христов, Х., Доклад на тема: „Фирменото контраразузнаване н действие”, Научна конференция „MATTEX 2014”, проведена в ШУ „Еп. Константин Преславски” на 22-22.11.2014 г., докладът е публикуван в сборник научни трудове;

1.2.45.Христов, Х., Доклад на тема: „ПОДХОДИ ЗА СЪЗДАВАНЕ НА СИСТЕМА ЗА УПРАВЛЕНИЕ НА ФИРМЕНА СИГУРНОСТ ”, Годишник на Техническия факултет на ШУ „Еп. Константин Преславски”, 2014.

1.2.17. Стратегиите за противодействие на посегателства срещу бизнес организацията са научно обосновани и аналитично аргументирани и се реализират чрез последователно и системно прилагане на механизми и процедури за защита и контрол, насочени към ограничаване на негативното влияние на съществуващите заплахи и посегателства.

Докладът „Активна и пасивна стратегии за управление на противодействието на посегателства срещу бизнес организацията – предимства и недостатъци”, изследва вземането на решение за избор на стратегия за управление на противодействието на посегателства срещу социалната организация, като една от трудните управленски дейности, осъществявани в условията на сложна и динамично променяща се среда за сигурност.

Посочено е, че рационалният избор на алтернатива за действие на дадена социална организация в конкретна среда за сигурност се извършва въз основа на определяне на оптималния възможен брой алтернативи, между които се осъществява избора и на прилагане на система от критерии за сравнение на вариантите за действие.

1.2.18. Дефинирането на противодействието на посегателства и прилагането на подхода на управление на противодействието в сферата на фирмената сигурност е един от възможните механизми за повишаване ефективността на процеса по защита сигурността на бизнес организациите от съвременните предизвикателства. В тази връзка, в доклада „Аспекти на управлението на противодействието срещу посегателства на фирмената сигурност”, са изследвани, целесъобразността от прилагане на подхода на управление на процеса на противодействието и организацията на противодействието на посегателства срещу сигурността на фирмата, като изключително важен етап в процеса на управление на бизнес организацията, разглеждан като предпоставка за постигане на висока степен на обективност на анализа и оценката на незащитеността на организацията и създаване на условия за рационалност на процеса на организиране на противодействието.

1.2.19. В докладът „Фирмена сигурност – характеристики”, икономическата система на всяко общество е представена, че се състои от голям брой бизнес организации (фирми). Затова успешното, пълноценно и ефективно решаване на задачите, стоящи пред икономическата сигурност на всяка държава, зависи от резултативността на тяхната дейност.

Интегрирайки характеристиките на формулираните подходи за анализ на понятията фирмена сигурност и посегателства срещу фирмената сигурност, в доклада е направен извода, че фирмената сигурност е комплекс от взаимосвързани мероприятия и

дейности осъществявани в бизнес организацията с цел предотвратяване, разкриване и неутрализиране на различни заплахи и форми на посегателства.

1.2.20. Докладът „Стратегии за управление на противодействието на посегателства срещу бизнес организацията – теоретични подходи", изследва теоретичните предписания за четирите нива на избор на стратегии в критични ситуации и/или в ситуации, в които системата, за да постави под контрол рисковите фактори, способни да доведат до дестабилизация на нейното управление, до изтощаване на нейните материални, финансови, когнитивни и човешки ресурси и до нарастване на нейната несигурност.

В изследването са анализирани предимствата и недостатъците на две основни стратегии за организиране на противодействието срещу посегателства на фирмената сигурност – пасивна, т.нар. стратегия за вътрешна сигурност и активна, наречена в практиката стратегия за външна сигурност.

1.2.21. В доклада „Aspects of the organization for counteraction to attacks against the company security" са идентифицирани същността и смисъла на противодействието на посегателства срещу фирмената сигурност и връзката му с класическото контраразузнаване. Изведени и анализирани са видовете дейност, осъществявана от звената за фирмена сигурност в противодействието на посегателства срещу фирмена сигурност. Определени са възможните специфични сили, средства, способи и методи, използвани от звената за сигурност на бизнес организацията в противодействието на посегателства срещу фирмената сигурност. Формирано е становище за нормативната база, регламентираща функциите, целите, задачите и дейността на фирмените звена за сигурност, правните им възможности за ползването на средствата и методите на оперативно издирвателната дейност за защита на фирмената сигурност. Изградено е мнение относно взаимодействието между държавните и фирмените, по същество, оперативно-издирвателни служби, както и за възприемането на фирмената сигурност като елемент от защитата на националната сигурност.

1.2.23. Докладът„"Активната стратегия за управление на противодействието на посегателства срещу бизнес организацията – същност", изследва основно активната стратегия за организиране на противодействието срещу посегателства на фирмената сигурност, наречена в практиката стратегия за външна сигурност.

Изведена е тезата, че при активната стратегия на противодействие, бизнес организациите имат добре развита структура за сигурност, което ги поставя в категорията на добре защитените. Те си поставят за цел не само защита на собствените интереси, касаещи пасивната стратегия, но и придобиване на информация за средата, в която фирмата действа. При тях се създава организация за обработка на информацията още в суров вид, успоредно с процеса на нейното придобиване. И в този случай възложител и получател на разузнавателния продукт е службата за сигурност на компанията. Целта е готовият продукт да послужи за надеждното организиране на противодействието, целящо недопускане реализирането на посегателства срещу бизнес организацията. В известен смисъл, поради единство на процесите по сигурността, контраразузнавателната и разузнавателна дейност в тези компании се обединяват в един общ цикъл. Това се улеснява от създадената обратна връзка. Разгледани са и основните фактори, определящи последователността на предлаганата интегрирана проактивна стратегия на противодействие.

1.2.24. В доклада „Изучаване на социалната организация – елемент от организацията на противодействието на посегателства срещу фирмената сигурност", е посочено, че задълбоченото познаване на социалната организация, на нейната същност, мисия, цели, задачи е основна предпоставка за успешното дефиниране на активите за защита и идентифициране на уязвимостите на системата. Без наличието на

детайлна информация за всички функции и дейности на организацията, не може да се разчита на надеждно установяване на всички заплахи, произтичащи от организационната активност. Необходимо е наличие на задълбочено познаване на средата, в която оперира социалната организация. Притежаването на информация за основните характеристики на политическата, социална, законова и културна среда би позволило формирането на обективно познание за условията на функциониране на организацията и адекватно идентифициране на заплахите и посегателствата.

Принципното разглеждане на управлението на противодействието в сферата на сигурността, като компонент на стратегическото ръководство, определя необходимостта характеризирането на социалната организация да се осъществява в строго съответствие с развитието на стратегическата обкръжаваща среда.

1.2.27. В докладът „A model about organizing a counteraction to encroachments on company security", е предложен един възможен модел за организация на противодействието на посегателства срещу сигурността на фирмата, представен като изключително важен етап в процеса на управление на бизнес организацията, характеризиращ се със сложна съставна същност и включващ определени взаимно свързани дейности и процедури. Комплексното и прецизно осъществяване на всяка една от дейностите е предпоставка за постигане на висока степен на обективност на анализа и оценката на незащитеността на организацията и създаване на условия за рационалност на процеса на организиране на противодействието.

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; идентифициране на източниците на заплаха на дефинираните активи; идентифициране на уязвимостите на системата за сигурност на организацията; оценка на въздействието, което реализирали се заплахи оказват на организацията; оценка на незащитеността на организацията; анализ на съществуващите и планирани механизми, форми, методи и способи за противодействие и защита.

Комплексното разглеждане на посочените дейности е задължително условие за извършването на надеждно противодействие на посегателствата за организацията. Подценяването на някой от компонентите или непълното му характеризиране не би позволило извършването на надеждно идентифициране на посегателствата и би възпрепятствало осъществяването на последващите етапи от процеса на организация на противодействието.

1.2.32. В доклада идентифицирането на източниците на заплаха, се разглежда като съществена стъпка в процеса на противодействието на посегателства срещу организацията, насочена към оптимално идентифициране на реалните и потенциални източници на заплаха за социалната организация, детайлно определяне на техния произход, структура, характеристики и признаци за проявление. Тази стъпка е важна предпоставка за успешното осъществяване на систематизиране и приоритизиране на заплахите, в зависимост от степента на застрашаване сигурността на социалната организация, с цел адекватно организиране и прилагане на механизми за предотвратяване или неутрализиране на въздействието им.

За извършването на обективно идентифициране на заплахите, е необходимо да бъдат разгледани всички реални и потенциални източници на заплахи, които имат възможност да причинят вреди на социалната организация или съществуват в средата, в която тя функционира. В тази връзка са анализирани и изведени определения за същността и класификацията на източниците на заплаха.

1.2.36. В доклада „Passive strategy for management of counteraction to encroachments on business organization", е анализирана пасивната стратегия на противодействие на посегателства срещу организацията, при която се разчита на традиционните способи за физическа и персонална защита. Пасивната стратегия се реализира чрез комплекс от дейности за разкриване и противодействие на шпионажа и нелоялната конкуренция, пресичане на нерегламентиран достъп до фирмената тайна, установяване на вътрешнофирмен ред и прецизна работа с кадрите. Пасивната стратегия действа предимно във вътрешната среда. Изпълнението на всяка оперативна задача по линия на пасивната стратегия започва с преглед на условията за сигурност и доколко съществуващото положение удовлетворява настъпилите изменения вътре и вън от компанията. След това се прави преценка на уязвимостта по отношение на атаките от страна на конкурентите. В зависимост от изводите, се планират действия по тяхното неутрализиране. След като се приложат новите мерки за завишаване степента на защита, резултатите се докладват на ръководителя на службата за сигурност. Той преценява тяхната ефективност и доколко поставената задача може да се приеме за изпълнена на съответния етап. Това е първият етап от обратната връзка и той се осъществява в рамките на самата служба. След своята преценка, ръководителят на службата за сигурност докладва на ръководството на компанията за изпълнената задача. Висшият мениджмънт, от своя страна, оценява качеството на свършеното и доколко новите изисквания по вътрешната сигурност са приложими и не възпрепятстват технологичните процеси на отделните структурни звена. В зависимост от практическите резултати във времето, след известен период ръководството очаква преценка от службата по сигурност какви нови изисквания следва да се предявят в съответната област и това е съществения етап на обратната връзка в пасивния цикъл. Като правило, изискванията и инициативата за подобряване на вътрешните параметри на сигурността трябва да идват от службата за сигурност, а не от ръководството.

1.2.37. В доклада „APPROACHES ABOUT EVALUATION ON THREATS' INFLUENCE UPON SOCIAL ORGNIZATION", въз основа на направеното изследване на стратегиите за противодействие на посегателства срещу сигурността на организацията в доклада са направени следните изводи:

-Изследвайки стратегиите за противодействието на посегателства срещу фирмената сигурност, се навлиза в полето на научния мениджмънт. Това е така, защото дейностите по противодействието имат предимно практическа насоченост. Като такива, те подлежат на планиране, организиране, мотивиране и контролиране, тъй както всяка друга дейност, осъществявана във фирмата в качеството й на управленска система.

- Ефективното реализиране на стратегиите за управление на противодействието изисква осъзнаване на важността и разработване на научнообоснована управленска политика на стратегическото ръководство на бизнес организацията.

-Прилагането на активната стратегия на управление на противодействието в сферата на сигурността, фокусирана в етапа преди извършване на конфликтното взаимодействие, позволява реализация на своевременно и надеждно намаляване или елиминиране на вероятността източници на заплаха да въздействат на системата за сигурност на социалната организация.

1.2.38. Докладът „THE COMPANY SECURITY SYSTEM – A CONTRIVANCE TO COUNTERACT TO ALL POSSIBLE ENCROACHMENTS" е насочен към формиране на становище за същността на понятието „система фирмена сигурност", нейните структура и функции; определяне на системата за фирмена сигурност като общо средство за противодействие на всички възможни посегателства; определяне на видовете посегателства и техните възможни форми, методи и способи за реализиране, в контекста на необходимо условие за

организиране на ефективно противодействие. В главата са изследвани видовете посегателства срещу сигурността на фирмата, тяхната същност и етапи за реализиране.

1.2.39. Докладът „Подходи за дефиниране и оценка на ценностите и активите за защита на социалната организация“, предлага подход за определяне степента на незащитеност на социалната организация, за един от заключителните етапи на сложния процес на противодействие срещу посегателства и заплахи. Направена е оценка за нивото на незащитеност за организацията при наличие на определена двойка източник на заплаха – уязвимост. Определянето на степента на незащитеност е изразено като функция на: вероятността конкретен източник на заплаха да въздейства на конкретна уязвимост; магнитуда на неблагоприятно влияние при въздействие на източника на заплаха спрямо уязвимостите; степента на адекватност на планираните или прилагани механизми и процедури за защита, за намаляване или елиминиране на незащитеността.

За нагледно представяне на резултатите от измерване на незащитеността са изготвени матрици за нивото на незащитеността и скала на незащитеността с оценка на необходимостта от коригирането му. Матриците за нивото на незащитеността се изготвят въз основа на комплексното разглеждане на резултатите от оценка вероятността за проява на източника на заплаха и степента на негативния ефект от въздействието му.

1.2.40. Докладът „Подходи за оценка и анализ на незащитеността и механизмите за защита на социалната организация“, предлага подход за дефиниране и оценка на ценностите и активите за защита на организацията **за е**дин от основните етапи на противодействие на посегателства срещу сигурността на организацията. Посочени и анализирани са отделните компоненти на този етап, като се започва с направата на описание на обекта за защита (на организацията); да се определят елементите на системата и дейностите, които се извършват в тях; да се дефинират активите на организацията, които са обект на защита. Всеки актив трябва да отговаря на въпроса: „Защо се нуждае от защита и как той влияе върху цялостната сигурност на организацията?”. Приложима практика е извършването на „разрез на обекта за зашита”, като се опишат звената в организацията, в които съществуват активи за защита. „Първият момент в този етап се заключава в описване и оценяване на активите на организацията и определяне на техните собственици. За тази цел може да се приложи методика, базираща се на скала с условни единици, като се избегне конкретното парично остойностяване. Изборът на методиката следва да се извърши при отчитане на обекта за защита и спецификата на извършваната дейност”. Ценността на всеки актив се определя в зависимост от неговото значение за организацията и вида му. Необходимо условие за оценката на активите е да се извърши тяхната инвентаризация. При това те могат да се групират по видове, например: информационни активи, активи на програмното осигуряване, финансови активи, физически активи и услуги. На всеки актив се определя собственик, който да носи отговорност за ценностите.

1.2.43. В доклада „Фирменото контраразузнаване н действие”, е посочено, че посегателствата срещу фирмената сигурност се извършват с използване на конспиративни средства и методи. За да бъде успешно противодействието, то трябва да се извършва с използването на идентични средства и методи, а те по своята същност са контраразузнавателни (оперативни).

Анализът на направено изследване позволява да бъдат изведени следните заключения:

-Противодействието на посегателства срещу бизнес организацията от службите за фирмена сигурност се осъществява чрез видовете контраразузнавателна дейност, изразяваща се в разкриване, предотвратяване и пресичане на замислени

посегателства срещу фирмената сигурност, подпомагане на наказателното и административно производство и превантивна дейност.

-Като компонент на националната система за сигурност, бизнесът се нуждае от приемане на нормативна уредба, регламентираща функциите, целите, задачите и дейността на фирмените звена за сигурност, правните им възможности за ползването на средствата и методите на ОИД за защита на фирмената сигурност и взаимодействието със специализираните държавни институции.

1.2.45. Докладът „ПОДХОДИ ЗА СЪЗДАВАНЕ НА СИСТЕМА ЗА УПРАВЛЕНИЕ НА ФИРМЕНА СИГУРНОСТ ", защитава тезата, че защитата на бизнес организацията е функция на самата организацията като цяло и тя се осъществява от нейните структури за сигурност, в рамките на тяхната компетентност и в съответствие с възложените им функции и предоставените им сили, средства и методи на дейност. Обосновано е, че системата за сигурност на организацията е единствена форма за противодействие на различните форми на видовете посегателства. В този смисъл, службата за сигурност на организацията, се явява общото средство за противодействие на всички възможни посегателства. Службата за сигурност на едно търговско предприятие е организационната структура на системата му за фирмена сигурност, тя е материалният еквивалент на фирмената сигурност, като система. Тя има за основна цел да защитава фирмената сигурност, като използва своите специфични средства, методи и способи за превенция, разкриване, неутрализиране и подпомагане пресичането на дейността на онези вътрешни и външни сили, които извършват посегателства срещу бизнес организацията.

3.3.Стеганологична защита на информацията на социалната организация

1.2.11.Станев, С. и Христов, Х., Доклад на тема: „Предизвикателства на компютърната и мрежова стеганография към дейността на фирмените служби за сигурност", В: Сборник на юбилейна международна научна конференция на Департамент национална и международна сигурност, Тематично направление 3, НБУ, София, 2013;

1.2.12. Станев, С. и Христов, Х., Доклад на тема: „Роля на фирмените служби за сигурност при организиране на противодействието срещу стеганографски атаки", В: Сборник научни трудове на Университетска годишна научна конференция на НВУ „В.Левски", 2013, Научно направление „Сигурност и отбрана", В. Търново, 2013;

1.2.13.Станев, С., Христов, Х. и Диманова Д., Доклад на тема: „IT – стеганографията и новите предизвикателства към системите за сигурност", В: Сборник трудове на XI международна конференция „Сигурността в Югоизточна Европа – в търсене на интелигентни решения", Секция 2, София, 2013;

1.2.22.Stanev, S., Hristov, H., Dimanova, D., Доклад на тема: „Aproaches for stego defense of sensitive information from inside leakage", Journal Science education innovation, vol. 1, 2013;

1.2.28.Stanev, S., Hristov, H., Dimanova, D., „Approaches for stego defence of sensitive information", International Conference on Bionics and Prosthetics and Mechanicsq Mechatronics and Robotics, Volune 10, Latvia 2014, p. 117-123.

1.2.30.Zhelezov, S., Paraskevov, H., Hristov, H., Boyanov, P., „An architecture of steganological subsystem for information protection", International Conference on Bionics and Prosthetics and Mechanicsq Mechatronics and Robotics, Volune 10, Latvia 2014, p. 123-129.

1.2.32.Христов, Х., „Подходи за идентифициране на източниците на заплаха на организацията", Трета международна научна конференция –„Наука, образование, иновации", посветена на 145 годишнината на БАН и 35 годишнината от космическия полет на Георги Иванов, 21-23.05.2014 г., Шумен.

1.2.35. Христов, Х., „Стеганографските методи и конфиденциална информация в организацията – аспекти на атаки и защита”, Годишна Университетска научна конференция, НВУ „В. Левски”, 3-4.07.2014 г., В.Търново.

1.2.50. Илиев, Св., Христов, Х., Варна 2014 март - Стеганография - ВВМУ - "Курсантите и студентите на морско училище и науката" - 27.03.14г. Варна

1.2.51. Христов, Х., Досев, Н., Илиев, Св., Доклад на тема: „Възможности за използване на стеганография в социалните мрежи Facebook и Google+”, Трета международна научна конференция –„Наука, образование, иновации”, посветена на 145 годишнината на БАН и 35 годишнината от космическия полет на Георги Иванов, 21-23.05.2014 г., Шумен.

1.2.52. Христов, Х., Досев, Н., Илиев, Св., Доклад на тема: „Предаване на тайни съобщения чрез стеганографски методи и способи във Facebook и Google+”, Научна конференция „Новата парадигма за сигурност в киберпространството”, НВУ „В. Левски“ , Факултет „Артилерия, ПВО и КИС”, 5-6.06.2014 г.

1.2.53. Досев, Н., Илиев, Св., Христов, Х., „Възможности за секретна комуникация в социалната мрежа Google+”, Годишна Университетска научна конференция, НВУ „В. Левски”, 3-4.07.2014 г., В.Търново.

1.2.54. Димитров, Д., Илиев, Св., Христов, Х., „Възможности за секретна комуникация в социалната мрежа Facebook”, Годишна Университетска научна конференция, НВУ „В. Левски”, 3-4.07.2014 г., В.Търново.

1.2.11. Докладът „Предизвикателства на компютърната и мрежова стеганография към дейността на фирмените служби за сигурност”, защитава тезата, че вътрешните заплахи за социалната организация са особено трудно разрешим проблем, защото има много начини вътрешните зложелатели в организацията (т.н. „инсайдери”, от англ. insiders) да откраднат 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 своите компютърни 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.

1.2.12. Докладът „Роля на фирмените служби за сигурност при организиране на противодействието срещу стеганографски атаки”, посочва аспектите на заплахи от използването на компютърната и мрежова стеганография, и на защита срещу изтичане на конфиденциална информация чрез вътрешни за дадена организация нарушители и да се предлага система за наблюдение от страна на службите за сигурност на организацията, които да играят роля на защитни стени за мрежовия трафик. Актуалността на изследването е свързана с отговорностите на службата за сигурност на организацията при изграждането на ефективно противодействие на съществуващите възможности за използване на стеганографските методи за скрито извличане на конфиденциална информация от организацията. В изследването е въведено понятието „стегоинцидент”, характеризиращо реализирани посегателства (неправомерен достъп) на чувствителна за

организацията информация, свързани с използване на съвременните възможности на компютърната и мрежова стеганография.

1.2.13. В доклада „IT – стеганографията и новите предизвикателства към системите за сигурност", е анализирана 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.

Актуалността на доклада е свързана с отговорностите на службите за фирмена сигурност за ефективно противодействие на стеганографските методи за скрито извличане на конфиденциална информация.

Разяснено е как, с помощта на стеганографията инсайдери могат да предават извън зоните за сигурност на фирмата откраднатa секретна информация към Интернет, преодолявайки всички защитни филтри. За тази цел инсайдерите могат да използват някоя от над 1500 стеганографски приложения, достъпни в Интернет като безплатен (freeware) или shareware софтуер. Традиционните средства за мрежова сигурност и системи за предотвратяването на загуба на данни не откриват употребата на стеганография от вътрешни служители.

1.2.22. В доклада „Aproaches for stego defense of sensitive information from inside leakage", са маркирани и разгледани някои от комплекса от мерки за информационна сигурност. Това са обучение, виртуализация на рискови приложения, мрежова изолация и ограничаване на комуникациите , заглушаване с генератор на бял шум на зоната, в която се обра-ботват важни данни, ограничаване ползването на мобилни телефони, ограничаване и контрол на достъпа до Интернет, създаване на проксисървър. Мрежова изолация, VPN за достъп до Интернет, whitelisting, sandboxing и на първо място морала, мотивацията и обучението на хората – тези методи ще предотвратят множеството атаки, в това число и изтичането на информация. В политиката за IT- сигурност на фирмата могат да бъдат включени правила за забрана на внасянето, тегленето и ползването на криптиращи и стеганографски програми за лични цели без разрешението на системния администратор; забрана за достъп до Интернет на компютри, в които се обработва чувствителна информация на компанията; забрана за презапис на данни върху информационни носители; забрана за ползване в зоните за сигурност на компютри с достъп до Интернет, извън компютърната мрежа на компанията; стеганализ на всички изходящи по официалния мрежов канал на организацията мултимедийни обекти, или тяхното „зашумяване" чрез вграждане на специални стеганалитични съобщения, с цел унищожаване на евентуално вградена секретна информация, и др.

1.2.28. Докладът „Approaches for stego defence of sensitive information", разглежда развитието с времето на методите за скриване на данни и стеганографията и възможностите да се очакват нови заплахи за скриване на информация. При осъществяване на своята дейност и при възникване на необходимост създателите на зловреден софтуер, престъпните организации, терористите и държавните организации прикрият своите криминални дейности. Не само вероятно, но и сигурно е, че те ще развият и използват нови методи на стеганографията и други авангардни методи. Анализа на получените резултати от изследването определят, очаквания за използване на модерни методи за скрито предаване на информация да се насочат към изчисленията в облак, виртуализацията, модерните поточни протоколи, метаданните и базите от данни, безжичните протоколи, смартфоните и таблети. Доклада е насочен към службите за

сигурност на социалните организации, с цел организиране на ефективно противодействие и готовност да посрещнат тези предизвикателства.

1.2.30. Докладът „An architecture of steganological subsystem for information protection", е насочен към изследване на същността на въвеждане на определение за стеганологична подсистема за защита на информацията (СПСЗИ). Тя е определена, като част от системата за защита на информацията (СЗИ), която е комплекс от мерки, реализирани от няколко подсистеми за защита – антивирусна, защитна стена, криптозащита и др. Крайната цел на въвеждането на подсистема за стеганологична защита на информацията е повишаване на ефективността на комплексната СЗИ на дадена организация (фирма). СПСЗИ е съвкупност от апаратни и програмни средства за защита на информацията в компютърните системи и мрежи чрез методите на стеганографията и стеганализа.

Посочено е, че специалистите използват термина стеганология, обхващащ два смислово противоположни компонента- стеганография и стеганализ. Стеганографията е научно-приложна област, съвкупност от технически умения и изкуство за начините за скриване на факта на предаване (наличие) на информация. Стеганализът изучава методите за разкриване на наличието на скрити съобщения с използването на стеганографски методи.

Разгледани са основните модули на СПСЗИ и някои от важните проблеми възникващи в процеса на проектиране и реализация.

1.2.35. В доклада „Стеганографските методи и конфиденциална информация в организацията – аспекти на атаки и защита",, на базата на сценария за Алис и Боб, с цел задълбочено изследване на проблема за възможните стеганографски канали за изтичане на конфиденциална информация и практическа насоченост на изследването, е предложен хипотетичен модел на атаката на разузнавателната служба на организация „Б", с използване на стеганографски методи срещу организация „А". Организация „Б" е инициатор на незаконно посегателство върху конфиденциална информация. Управлението на „Б" поставя задача на разузнавателното си звено от службата за фирмена сигурност, да придобие конфиденциални данни на организация „А". Изрично е поставено условието задачата да бъде изпълнена в условия на пълна конспиративност, без атакуваната организация да узнае за изтичането на информацията. Разузнавателното звено на „Б" поставя изпълнението на задачата на своя служител – агент Боб.

Като конкретни мерки, заложени в политиката за IT-сигурност на организацията могат да бъдат посочени:

- забранана внасянето, качването, тегленето и ползването на криптиращи и стеганографски програми за лични цели без знанието и разрешението на системния администратор;
- забрана за достъп до Интернет на компютри, в които се обработва конфиденциална информация на фирмата, и забрана за презапис на данни върху информационни носители;
- забрана на наличието в зоната за сигурност на компютри с достъп до Интернет, извън компютърната мрежа на компанията;
- забрана на внасянето на лични компютри и мобилни апарати в зоните за сигурност на организацията с възможности за достъп до интернет;
- организиране на контрол върху изходящия трафик на компанията чрез проксисървър, защитна стена и др.;
- създаване на междинно звено, обслужващо проксисървъра с възможности за заглушаване на всички свободни интернет услуги;

- създаване на сървър за отстраняване на мултимедийни файлове и ограничаване възможността на служебния канал за прикачване на мултимедийни файлове;
- стеганализ на всички изходящи по официалния мрежов канал на защитаваната компания мултимедийни обекти, предавани в канала или тяхното зашумяване чрез вграждане чрез стегопрограми на специални стеганалитични съобшения, с цел унищожаване на евентуално вградена секретна информация.

1.2.50. Целта на доклада „Стеганография“ е запознаване с основните понятия в наука стеганография, както и новите достижения от последните години. Прието е определението, че стеганографията е изкуство и наука за предаване на тайни съобщения, чрез специални способи и средства. Антагонист на стеганографията е стегоанализът, който има за цел да открива тези съобщения. Предаването на информация е с ключово значение в днешното разбиране за сигурност. Запознаването със стеганографията и нейните достижения е задължително за всеки специалист занимаващ се със сигурност.

1.2.51. Докладът „Възможности за използване на стеганография в социалните мрежи Facebook и Google+”, изследва възможностите на социалните мрежи, за използването на стеганография в тях. Целта е да се разкрие част от заключенията и резултатите, до които авторският колектив стигна по време на изследванията. Представени са възможностите за споделяне в две от най-разпространените социални мрежи – Facebook и Google+. Направени са препоръки и са очертани насоки към бъдещи изследвания по въпроса.

1.2.52. В доклада „Предаване на тайни съобщения чрез стеганографски методи и способи във Facebook и Google+”, престъпниците от ново поколение, които интегрират технологиите в своите криминални дейности, могат да използват възможностите, които предоставят социалните мрежи, по същите начини, които използват частните или юридически лица. Стеганографията в социалните мрежи, дава възможност за тайно комуникиране, предаване на файлове, легално съхранение на информация в тях и др.

Експериментът доказа, че рутинността, която са добили социалните мрежи в своето използване, се явява проблем, пред защитата от използване на стеганографски способи. Един от основните белези, е че използването на социалните мрежи за споделяне на снимки и друг вид файлове, е нещо съвсем нормално в днешно време и не буди подозрения. Още един факт, който подкрепи нуждата от изследване на възможностите за стеганография в социалните мрежи е, че тези методи могат да бъдат използвани от хора без специализирано техническо образование. В заключение може да се каже, че опасността от тайно комуникиране в социалните мрежи е напълно реална.

1.2.53. Изследването в доклада „Възможности за секретна комуникация в социалната мрежа Google+” доказа, че е възможно използването на стеганография в социалните мрежи. Това твърдение обаче, има някои ограничения относно Facebook. Стеганография, чрез прикрепянето на данни към „контейнер“ и споделянето му във Facebook или Google+, е напълно възможно и реално. Проблемът, които се появява при Facebook е извличането на скритото съобщение, в следствие обработка на снимката, но все пак има възможност за използването на платформата. Новата опция за споделяне на файлове във Facebook, е тайната вратичка, която би могла да се използва за предаване на „контейнери“. Файловете могат да бъдат от всякакъв формат, стига той да не е .mp3 или .exe и да влизат в ограничението за размер – 25 MB.[5] Експеримента установи, че SteganographyStudio и BPMSecrets, могат да предадат „контейнер“ със стеганографска информация, а SilentEye също позволява извличането на тайното съобщение, но трябва да се отбележи, че снимката променя коренно своето качество. Толкова явна манипулация на снимка, непременно би породила съмнение.

1.2.54. От получените резултати на направеното изследване в доклада „Възможности за секретна комуникация в социалната мрежа Facebook”, могат да се направят няколко извода:

- Google+ е изключително атрактивна мрежа що се отнася до предаване на тайни съобщение, чрез стеганографски техники.
- JPEG и BMP се приемат успешно като формати, които могат да се използват за „контейнери“.
- Използваните стеганографски софтуери BMPSecrets, Steganography Studio и SilentEye са успешно приложими в Google+.
- Фактът, че размера на качените и свалените изображения е абсолютно един и същ, както и съвпадението на MD5 стойностите при качване и сваляне, говори за абсолютна никаква манипулация върху изображенията, от страна на платформата, при тяхното споделяне.

3.3.Защита на личните данни на социалната организация.

1.2.10. Станев, С. и Христов, Х., Доклад на тема: „Стеганографските методи и личните данни – аспекти на атаки и защита”, В: Сборник трудове на научна конференция „Защитата на личните данни в контекста на информационната сигурност”, Секция Информационна сигурност, Факултет „Артилерия, ПВО и КИС” на НВУ, Шумен, 2013;

1.2.14. Христов, Х., Доклад на тема: „Защита на личните данни – елемент от системата за сигурност на организацията”, В: Сборник научни трудове на Университетска годишна научна конференция на НВУ „В. Левски”, 2013, Научно направление „Сигурност и отбрана”, В. Търново, 2013;

1.2.15. Христов, Х., Доклад на тема: „Посегателства срещу лични данни в организацията – специфични аспекти”, В: Сборник трудове на научна конференция „Защитата на личните данни в контекста на информационната сигурност”, Секция „Държава и сигурност”, Факултет „Артилерия, ПВО и КИС” на НВУ, Шумен, 2013;

1.2.16. Христов, Х., Доклад на тема: „Защита на личните данни – обективна необходимост в организацията”, В: Сборник трудове на научна конференция „Защитата на личните данни в контекста на информационната сигурност”. Секция „Държава и сигурност”. Факултет „Артилерия, ПВО и КИС” на НВУ, Шумен, 2013.

1.2.10. Информацията за личните данни е един от обработваният от информационните системи на организаците компонент. Тези данни могат да са обект на посегателства от фирми и групировки. За целите си те използват различни методи, включително и нови информационни технологии за проучвателните дейности, информационни атаки, информационни и психологически въздействия. В тази връзка в доклада „Стеганографските методи и личните данни – аспекти на атаки и защита”, е изследвано едно от ефикасните направления за създаване на скрити канали за изтичане на информация 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. Посочено е ,че стегопрограмите могат да се прилагат както за целите на защитата на данните, така и за незаконни цели - за изтичане на чувствителна информация за хората.

Посочена е и анализирана нормативната уредба регламентираща работата и защитата на правата на физическите лица при обработването на личните данни. Разгледани са аспектите на тази защита в частния сектор, и преди всичко на борбата срещу новите методи за информационна престъпност.

2.2.14. Докладът „Защита на личните данни – елемент от системата за сигурност на организацията”, разглежда организацията на защитата на личните данни в социалната организация. Дадени са различни определения за личната и обществената сигурност. Понятието сигурност се формулира като безопасност и защитеност на обществената формация или индивид, осигуряващи съхранението и развитието им. Следователно, незащитеността и посегателствата на личните данни кореспондира пряко със сигурността на индивида и организацията. Посочено е ,че е не може да бъде разработена система за защита на личните данни за конкретна организация, без да са разкрити и анализирани конкретните форми и способи на посегателствата. Обратният подход би бил дълбоко концептуално погрешен и води до абсолютно неадекватна на действителността система за защита. В организацията администраторът на лични данни предприема необходимите технически и организационни мерки, за защита на данните от случайно или незаконно унищожаване, или от случайна загуба, от неправомерен достъп, изменение или разпространение, както и от други незаконни форми на обработване. Администраторът е длъжен и да вземе специални мерки за защита, когато обработването включва предаване на данните по електронен път

2.2.15. В доклада „Посегателства срещу лични данни в организацията – специфични аспекти”, е посочено ,че посегателствата срещу личните данни са обективно съществуващи в действителността негативни обществени явления. Проявлението на конкретни форми и способи в действителността зависи от волята на инициатора. Формите и способите на видовете посегатества не са абстрактни понятия, а конкретни понятия – имат своите индивидуализирани субекти (инициатори), ясен предмет на посегателство (лични данни), реализира се определен и съзнателно търсен от инициатора резултат.

В тази връзка посегателствата срещу личните данни стават част от оперативната среда на бизнес организациите. Това е нещо, от което нито един собственик не може да избяга. Мениджърите все по-ясно разбират значението на запазването на своите вътрешни секрети и последиците от несанкциониран достъп на терористични организации и чужди разузнавателни сили до тях. Несигурността за бъдещето на организацията пряко кореспондира с изпреварващото определяне и предвиждане на възможни заплахи и посегателства за личните данни на организацията.

2.2.16. 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. Целта на изследването в доклада „Защита на личните данни – обективна необходимост в организацията”, е да се разкрият възможностите за използване на класическите контраразузнавателни методи и способи за противодействие на каналите за изтичане на конфеденциална информация /каквито са личните данни/ от вътрешни за дадена организация нарушители, и да се предложи активна система за наблюдение от страна на службите за сигурност на организацията.

4. Ръководител на дипломанти за периода от 2007 до 2012г.:

1. ДП на тема: **„**Стеганографски методи за защита на информацията в социалните мрежи **",** дипломант Светлин Пламенов Илиев Ф № 1070070010/ТСС0044/, бакалавърска програма: в направление: 9.1. Национална сигурност, специалност Системи за сигурност, юли 2014г.

2. ДП на тема: **"** Стратегия за управление на риска от корупция за МО и БА **",** дипломант Станислав Павлов, Ф № 1472111004 магистърска програма в направление: 9.1. Национална сигурност, специалност Системи за сигурност, юли 2014г..

3. ДП на тема: **„**Стратегия за управление на риска от корупция за МО и БА **",** дипломант Полина Тошкова Маринова Ф №1170070019 бакалавърска програма в направление: 9.1. Национална сигурност, специалност Системи за сигурност, юли 2015г.

4. ДП на тема: **„**Организираната престъпност – заплаха за националната сигурност **",** дипломант Мартин Марчев Чобанов, Ф№1170070006, бакалавърска програма в направление: 9.1. Национална сигурност, специалност Системи за сигурност, юли 2015г.

Обобщена справка за публикациите представени за рецензия на конкурса

№ по ред № по ред	Характер на труда	Всичко	
		количество	обем (стр.)
	I. Трудове по номенклатурната специалност.		
1.	А/ *Монография*.	1	264
2.	Б/ *Учебници и учебни пособия*.		
	- Учебници.	3	495
3.	Б/ *Публикации в периодични научни списания и изнесени научни доклади*.		
	- Научно-теоретични статии.	13	104
	- Доклади на научни сесии и конференции.	24	176
	- Съвместни доклади със студенти.	12	72
	III. Научно-изследователски разработки, рационализаторска и внедрителска дейност.		
	А/ Научно-изследователски разработки.		
	- участие в национален проект;	3	
	- участие в университетски проекти.	4	
	- Участие в други университетски проекти не финансирани от Шуменския Университет	2	
ВСИЧКО:		**71**	**1111**

Изготвил:…… ….
/гл.ас. **д-р Хр. Христов/**