КЛАСИЧЕСКИ И СЪВРЕМЕННИ ИЗМЕРЕНИЯ НА ИНДУСТРИАЛНИЯ КОНТРАШПИОНАЖ

д-р Цанко Иванов
Експерт по корпоративна сигурност и конкурентно разузнаване

Резюме

Настоящият доклад представя различен поглед към класическите и съвременни измерения на индустриалния контрашпионаж в контекста на прехода от информационно към познавателно общество. Изведени са различни заплахи за интелектуалната собственост с цел откроряване на засилващото се значение на сигурността в съвременните предприятия.

Ключови думи: индустриален контрашпионаж, корпоративна сигурност, заплахи.

CLASSIC AND MODERN ASPECTS OF INDUSTRIAL COUNTERESPIONAGE

Tsanko Ivanov, PhD
Corporate Security and Competitive Intelligence Expert

Abstract

The author of the report introduces a different view on both classic and modern aspects of industrial counterespionage in context of the transition from information to knowledge society. Different threats to intellectual property have been identified in order to highlight the increasing role of security in modern business.

Key words: industrial counterespionage, corporate security, threats.

„Събирането на икономическа, научна и технологична информация става част от съвременната бизнес култура.” ~ Адмирал Пиер Лакост[1]

В съвременния свят, белязан от безпрецедентни геополитически, икономически, социални и технологични промени, фирмената и националната конкурентоспособност все повече зависят от способ-

[1] Бояджиев, Т. Изповед на шпионина. София: Сиела, 2018, с. 12.

ността на компаниите да извличат полза от научно-изследователски достижения и иновации. Краят на Студената война, развитието на информационните технологии и ограничените ресурси за вътрешнофирмени разследвания при кражби на търговски тайни са причини индустриалният шпионаж да се превръща във все по-печелившо начинание.[2] Предпоставки за това са и новите възможности, които свързаните с индустрия 4.0 комуникационни и информационни технологии предоставят на новото поколение кибер престъпници, за които дори държавните граници вече не представляват сериозна пречка. В допълнение, в науката и практиката по корпоративна сигурност през последните години все повече се завишава значението на вътрешните за компаниите заплахи и необходимите контрамерки като кибер/комуникационна сигурност, бизнес континуитет, вътрешнофирмени разследвания, превенция и др.[3]

Целта на настоящия доклад е да открои най-честите методи и способи за посегателства над интелектуалната собственост на съвременните предприятия като паралелно с това систематизира различни класически и съвременни измерения на индустриалния контрашпионаж. Авторът проследява тъмната страна на икономическите и социалните промени, до които води развитието на новите технологии и засилването на свързаността в глобализиращия се свят. Актуалността на проблематиката се дължи още на едновременното желание на бизнеса да споделя чувствителна информация с подходящите заинтересовани страни с цел засилване на конкурентни позиции, от една страна, и защита на същата информация от други партньори, доставчици, клиенти, конкуренти, чужди правителства, криминален контингент и т.н., от друга.

---

2 Nasheri, H. (2005) *Economic Espionage and Industrial Spying.* NY: Cambridge University Press, p. 8.

3 На база ежегодни изследвания в областта на корпоративната сигурност в САЩ на американската компания Securitas Security Services. За повече информация: Walker, D. & Co. (2017) *Top Security Threats and Management Issues Facing Corporate America: 2016 Survey of Fortune 1000 Companies.* Parsippany, NJ: Securitas Security Services Inc., p. 7.

Разграничаване на използвания понятиен апарат

Някои изследователи и експерти слагат знак за равенство между понятията *икономическо разузнаване, конкурентно разузнаване* и *индустриален (промишлен) шпионаж*, но този подход не е коректен. Икономическото разузнаване представлява допълнение към политическото и военното разузнаване като по-голямата част от разузнавателните сведения са от открити източници.[4] Чрез него се цели придобиване на информация за конкретни компании, но и обща икономическа информация за съответната държава с високо равнище на обобщаване.[5] Икономическо разузнаване се ръководи и спонсорира от отделните национални правителства за генериране на финансово-икономически ползи на държавно ниво чрез упълномощените за това компетентни служби за външно разузнаване.

Конкурентното разузнаване включва постоянен процес на легална частна разузнавателна дейност за придобиване на оперативна информация относно средата, в която функционират предприятията, с цел оптимално и своевременно информационно обезпечаване на процеса на вземане на стратегически решения.[6] С други думи, конкурентно разузнаване е напълно легален елемент на системата за сигурност в съвременните предприятия и представлява добре балансиран инструмент за ранно предупреждение.

Промишленият (отначало известен като търговски) шпионаж има за цел събиране на сведения извън законно установените средства. От 80-те години на миналия век терминът се използва по отношение на държавно шпиониране между две страни с традиционните тайни методи.[7] В специализираната литература се използва и до-

---

[4] Полмър, Н. и Т.Б. Алън. Енциклопедия на шпионажа. София: Труд, 2001, с. 232.

[5] Василев, Е. Фирмена сигурност: Нелоялна конкуренция и фирмен контрашпионаж. София: Труд, 2000, с. 38-39.

[6] Начев, Й. Конкурентно разузнаване. София: Сиела, 2007, с. 55.

[7] Полмър, Н. и Т.Б. Алън. Енциклопедия на шпионажа. София: Труд, 2001, с. 474.

пълнителна класификация, например:

- *индустриален шпионаж* – търсене и придобиване на фирмени тайни главно от производствени и изследователски звена на предприятията;
- *бизнес шпионаж* – прилаган в сектора на услугите, главно в търговски и маркетингови отдели на компаниите;
- *корпоративен шпионаж* – събирателен термин, обединяващ всички свързани с понятието незаконни методи и практики в икономическа и бизнес среда.

В настоящия доклад терминът индустриален шпионаж се използва в смисъла на класическо корпоративно престъпление, т.е. събиране и използване на информация (вкл. посегателства срещу интелектуалната собственост) от една компания-конкурент срещу друга по незаконен и/или неетичен начин, породено от частни икономически интереси. В допълнение, свързаните незаконни практики са насочени към най-високо ниво фирмени тайни, служебни бази данни, вкл. разработени разузнавателни информационни продукти от конкурента, патенти и т.н. с цел незаконното им придобиване. Въпреки всички изброени негативи, най-сериозният е стремежът към потайност и незасичане на шпионските дейности за дълги периоди от време, през които атакуваните компании нямат отговор за отслабеното си представяне на съответния пазар.[8]

Интелектуалната собственост представлява търговска тайна и обект на правна защита като в американската нормативна рамка е залегнала следната дефиниция: „всички форми и видове финансова, бизнес, научна, техническа, икономическа или инженерна информация, включваща модели, планове, компилации, програмни устройства, формули, дизайни, прототипи, методи, техники, процеси, процедури, програми и кодове, независимо дали са веществени или не и независимо от начина за съхранение и запаметяване – физичес-

[8] Grooms, Th. F. (2016) *Market Intelligence… The Original Work.* CreateSpace Independent Publishing Platform, 1st Edition, pp. 147-149.

ки, електронен, графичен, фотографски или писмен, ако: А) собственикът е взел адекватни мерки да запази информацията в тайна и Б) информацията може да доведе до реални или потенциални икономически ползи, които още не са известни за обществото."[9] В националното законодателство постановките не са много по-различни като под производствена или търговска тайна се разбира „факти, информация, решения и данни, свързани със стопанска дейност, чието запазване в тайна е в интерес на правоимащите, за което те са взели необходимите мерки."[10]

Методи и способи за посегателства над интелектуалната собственост

В нередки случаи през последните години, конкурентната борба приема форма на конкурентна война, в която загубилите престават да бъдат част от пазара. В „шпионските игри" между корпорации и държави, особено в контекста на индустрия 4.0, се разрастват и усложняват използваните средства за нелегално и неетично придобиване на поверителна за компаниите информация. Основно слабо звено в системите за корпоративна сигурност на предприятията продължава да бъде човешкият фактор като мотивиращите причини за това са многобройни. Сред тях неизменно присъстват патриотизъм, парични стимули, идеология (политическа, социална или религиозна), его, задлъжнялост и други разнообразни методи за изнудване и оказване на натиск като пристрастеност към упойващи вещества, притежание на видео или снимков материал, включващ сексуални контакти, предишни кражби и т.н. В таблица 1 са систематизирани и основните обекти на атака в компаниите, разделени по различни признаци:

---

9 18 U.S.Code §1839(3): https://www.law.cornell.edu/uscode/text/18/1839

10 Закон за защита на конкуренцията: изм. ДВ. бр.7 от 19 Януари 2018 г., точка 9 от § 1 от допълнителните разпоредби. Достъпно на: http://www.lex.bg/bg/laws/ldoc/2135607845

Таблица 1

Групиране на обектите на индустриален шпионаж и конкурентно разузнаване

Най-често атакувани търговски тайни	Най-атакувани индустриални сектори	Най-атакувани активи
Клиентски списъци	Фармацевтичен	Формули
Информация за цени и разходи	Химически	Патенти
Научна и изследователска информация	Хранително-вкусов	Патентовани програми и процеси
Информация за продажбите	Софтуерен	Устройства
Информация за производството	Аерокосмически	Методики
Стратегически планове	Автомобилен	Техники

Източник: Fink, S. (2002) Sticky Fingers: Managing the Global Risk of Economic Espionage. Chicago: Dearborn Trade Publishing, pp. 266-267.

В допълнение, професионалистите в областта систематизират четири големи групи слаби места в компаниите[11], включващи:

- **Операционни слаби места –** социален инженеринг, несигурен интернет достъп, работа вкъщи или навън и др.
- **Физически слаби места –** лесен достъп до сгради и съоръжения, слаб или липсващ контрол над служебната информация, липса на пароли за достъп, липса на разписани протоколи за сигурност и др.
- **Слаби места, свързани с персонал –** липса на проучвания за служители, вътрешни престъпления, стрес, финансова задлъжнялост и др.
- **Технически слаби места –** зловреден софтуер, вируси, хакерски атаки, лесно пробивани пароли и др.

Изброените многобройни методи и инструменти за съвременен шпионаж в предприятията изискват необходимите контрамерки за опазване на тяхната интелектуалната собственост.

[11] Winkler, I. (1997) *Corporate Espionage.* Rocklin, CA: Prima Publishing.

Същност и измерения на индустриалния контрашпионаж

Независимо кой от описаните по-горе способи за атака се използва срещу предприятието, неговата системата за сигурност трябва да е способна да отговори на всички тях, защото често кражбите на интелектуална собственост са прикрита форма и на държавно ръководен икономически шпионаж. Следователно, като неизменен елемент от мрежата за сигурност в предприятията, трябва да присъства и звено за индустриален контрашпионаж. Няма единна дефиниция на това понятие, но то задължително включва „серия от проактивни мерки и мероприятия, възприети от бизнеса за идентифициране и неутрализиране на реални и потенциални заплахи към неговата интелектуална собственост както от собствени служители (вкл. пенсионирани, напуснали, уволнени и служители по заместване, консултанти и други лица с временен достъп – стажанти, гости, журналисти и т.н.), така и от конкурентни разузнавачи на друга компания или държава."[12]

Измеренията на индустриалния контрашпионаж са антипод на действията, типични за икономическото разузнаване, конкурентното разузнаване и корпоративния шпионаж. С други думи, те целят опазване на интелектуалната собственост на компанията от всякакъв вид атаки – както напълно легални, така и незаконни и/или неетични. От тази гледна точка, понятието коректно може да се използва като синоним на корпоративно контраразузнаване, осигуряващо активно и реактивно идентифициране и неутрализиране на широк кръг заплахи, произтичащи от конкурентни разузнавателни дейности с цел облага.[13]

За пълно възприемане и изпълнение на контраразузнавателни задачи е необходимо предприятията да преодолеят две огромни

---

[12] Иванов, Ц. В. Модел на система за активна корпоративна сигурност в индустриалните предприятия в Република България. Дис. Варна, 2018.

[13] Bernhardt, D. (2003) *Competitive Intelligence: How to acquire and use corporate intelligence and counter-intelligence.* London: Pearson Education Ltd., pp. 85-89.

заблуди, свързани с индустриалния шпионаж: първо, че той представлява реална опасност само за големи предприятия или ТНК и второ, че с контрамерки, актуални за Индустриалната ера може да се противодейства на заплахите от Информационната ера.[14] В опит за опровергаване на тези противоречия, чрез емпирично изследване относно нивото на сигурност и заплахите пред предприятията в българската химическа индустрия, проведено през 2017 г., авторът успява да събере и анализира голям брой количествени и качествени данни с помощта на анкетно проучване сред реално функциониращи индустриални предприятия и дълбочинни интервюта с настоящи и бивши ръководители, оперативни служители и експерти от МВР, ДАНС, МО, частни компании за сигурност и академични звена. Резултатите от него потвърждават изводите в теорията по проблематиката за ролята на индустриалния контрашпионаж като активно мероприятие в осигуряването на функцията по сигурност в предприятието.[15] Факторите за това са няколко:

- индустриалните предприятия са чест обект на промишлен шпионаж заради спецификата на производствените процеси, постоянното развитие на технологиите, брой на патенти и полезни модели, характер на интелектуалната собственост и т.н.;

- търсените от нелоялен конкурент или икономически шпионин ползи могат да са причина за изключително сериозни за предприятието дългосрочни щети;

- подобни нелоялни и незаконни практики трябва да се неутрализират от напълно интегрирано в системата за корпоративна сигурност звено за индустриален контрашпионаж.

В следващите параграфи са изведени част от възможните класически и съвременни методи, подходи и инструменти при осигуря-

---

[14] Burgess, Cr. & R. Power. (2008) *Secrets Stolen, Fortunes Lost: Preventing Intellectual Property Theft and Economic Espionage in the 21st Century*. Syngress Publishing, p. xiii.

[15] За допълнителна информация: Иванов, Ц. В. Модел на система за активна корпоративна сигурност в индустриалните предприятия в Република България. Дис. Варна, 2018.

ване на функцията по индустриален контрашпионаж в предприятията.

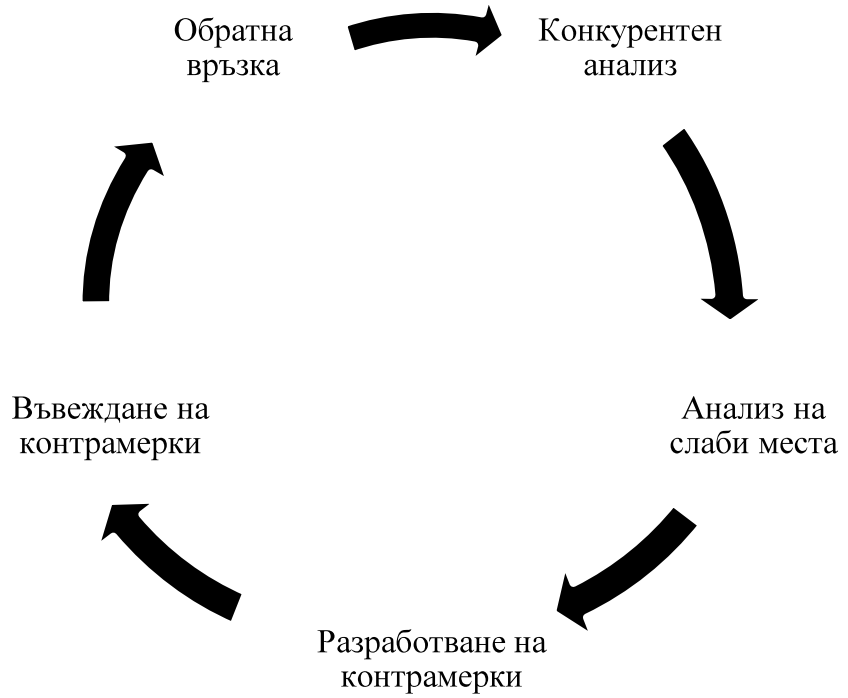
Класически измерения

Класическите подходи при осигуряване сигурността на интелектуалната собственост са свързани както с чисто физически пасивни мерки за сигурност, така и с някои активни мероприятия като:

- Предотвратяване на всякакъв род кражби, измами и злоупотреби;
- Предотвратяване на внедряване на лица, наети от нелоялни конкуренти и други вредоносни субекти;
- Извършване контрол на достъпа;
- Наблюдение с технически средства, пожарна безопасност и сигнално-охранителна техника;
- Изграждане на формални и неформални отношения със служители на предприятието от всички звена;
- Изграждане на формални и неформални отношения с колеги от сходни звена на лоялни конкуренти;
- Изграждане на формални и неформални контакти със служители от държавните правоохранителни органи и с представители от други публични институции;
- Изграждане/използване на доверителни отношения с представители на криминалния контингент с цел постоянно наблюдение на престъпните практики в отрасъла;
- Мерки за опазване на вътрешнофирмени тайни и различни видове индустриална собственост като патенти за изобретения и полезни модели, търговски марки и услуги, ноу-хау и др.;
- Защита на всички комуникационни канали, по които се пренася вътрешнофирмена информация – телефонни, интернет и интранет системи;

- Планиране, организиране и ръководене на секретно деловодство за съхранение на документи и друга поверителна информация, записана на физически носители;
- Разработване, утвърждаване, прилагане и контрол на вътрешни нормативни актове;
- Обучения при постъпване на работа в предприятието и регулярни обучения на персонала.

В обобщение на изведените мерки, те биват имплементирани в четирите нива на класическия контраразузнавателен цикъл, включващ: 1) разработване на контраразузнавателна прогноза; 2) провеждане на контраразузнавателни проучвания; 3) разработване на контраразузнавателен план; 4) приложение на подходящите контраразузнавателни мерки.[16] В бизнес среда, контраразузнавателният цикъл приема измеренията, посочени на фигура 1:



Фиг. 1. Класически бизнес контраразузнавателен цикъл

[16] U.S. Marine Corps (2007) *Counterintelligence.* NY: Cosimo Reports, Inc., p. 1-5.

Фигурата е адаптирана от автора на база собствен опит, специализирана литература по темата и възможното практическо приложение

Съвременни измерения

Съвременните практики в сферата на индустриалния контрашпионаж са свързани главно с осигуряване на кибер сигурността на предприятието[17] и някои други проактивни мерки на системата за сигурност, вкл.:

- Събиране и анализ на информация за потенциални нелоялни конкуренти и други рискови обекти;
- Дезинформиране на нелоялен конкурент;
- Ограничаване на информацията, публикувана в сайта на компанията, персонални профили в социалните мрежи и др.п.;
- Намаляване на риска от социален инженеринг[18] – водеща е идеята, че дори наглед маловажна информация може да се окаже сериозно оръжие в ръцете на неподходящите хора;
- Намаляване на риска от електронно подслушване чрез софтуерни решения, контранаблюдение и т.н.;
- Провеждане на стрес тестове – широко препоръчвани с цел получаване на актуална информация за собствената ефективност на звеното за контрашпионаж;
- Подобряване на базовата сигурност – мерки, свързани с цялостната сигурност, предприемани преди гореописаните като регулярен мониторинг на звената, осигуряващи физическата сигурност, контрола на достъп в предприятията, защитата на различните активи и др.

---

[17] Систематизираните подходи са заимствани от: Allsopp, W. (2009) *Unauthorized Access: Physical Penetration Testing for IT Security Teams.* Wiley, p. 248.

[18] Класически способ за атака на конкурентна компания, представляващ възможност за манипулиране на служители с крайна цел получаване на вътрешна информация – имена, адреси, телефонни номера, пароли и др.п. За повече информация вж.: Mitnick, K. (2003) *The Art of Deception*. Wiley. pp. 164-165.

Таблица 2

Обхват на мерките, свързани с индустриалния контрашпионаж

Мерки	Съдържание и обхват
Идентифициране	Откриване на рискове и заплахи от шпионаж както с човешки, така и с технологичен характер
Внезапни проверки	Проактивно премахване на рискове и заплахи от шпионаж както с човешки, така и с технологичен характер
Корпоративна сигурност/Безопасност	Реактивни действия при вече настъпили вредоносни последици за предприятията
Разследвания / Специални операции	Превантивни или последващи оперативни дейности с цел откриване на вредоносния обект (крадец, програма, вирус, конкурентна компания, чужда специална служба и др.)
Наблюдение / Контранаблюдение	Превантивни или последващи оперативни дейности, свързани със засилен мониторинг на външната и вътрешната среда на предприятията
Осведоменост / Обучения / Корпоративна култура	Провеждане на обучения сред мениджъри, акционери, служители, стажанти, медии, клиенти, партньори, доставчици, граждани и др. заинтересовани лица по въпросите на превенцията на опасни и агресивни шпионски активности

Източник: Grooms, Th. F. (2016) Market Intelligence… The Original Work. CreateSpace Independent Publishing Platform, 1st Edition, pp. 157-159

В таблица 2 са представени основните групи мерки, свързани с индустриалния контрашпионаж, както и тяхното съдържание. Те са логичен резултат от еволюцията в западния бизнес модел да се търсят пресечни точки между национални и корпоративни програми за икономическа сигурност.[19]

Началото на XXI век бе белязано от изключителен технологичен подем. Съвсем аргументирано може да се заключи, че човечест-

[19] Повече информация по темата може да се намери в многобройни западни публикации по темата, например „Националната контраразузнавателна стратегия на САЩ за 2016 ” и „Стратегически план 2018-2022”, публикувани от Център за контраразузнаване и сигурност към Офиса на Директора на националното разузнаване на САЩ.

вото премина от Индустриалната в Информационната епоха и уверено продължава към Познавателната епоха. За съжаление, в света на бизнеса подобни преходи не носят само позитиви в лицето на подобрени методи за комуникация, различни иновации, интелигентни производствени процеси и др. Човешката алчност, растящото неравенство и други фактори предоставят възможност за нов вид криминални и неетични активности спрямо бизнеса, за които нито отделните предприятия, нито службите за сигурност успяват да отвърнат подготвено. Технологичните достижения, развитието на мобилните приложения и др.п. прави икономическия и корпоративния шпионаж едновременно много по-лесен и по-евтин. Следователно, противодействието на различни посегателства към интелектуалния капитал на предприятията трябва да е обща задача както за засегнатите компании, така и за техните правителства, защото икономическия просперитет на една държава е основен фактор и при осигуряването на нейната сигурност. От тази гледна точка границите между национална и корпоративна сигурност все повече се размиват.

Представените в настоящия доклад подходи, методи и инструменти за индустриален контрашпионаж далеч не изчерпват широкия кръг дейности, от които заетите с тази дейност експерти биха могли да се възползват. Нито още по-големия брой сценарии, по които предприятията могат да бъдат застрашени. Новото хилядолетие носи със себе си и нов вид, много трудни за засичане и неутрализиране заплахи, срещу които е необходимо да се изгради сложна система за сигурност в предприятията. Подобен подход продължава да бъде подценяван от мениджмънта, най-често заради финансовата тежест, която носи. Финансовите загуби от евентуален пробив в сигурността, обаче, могат да се окажат още по-вредоносни в дългосрочен аспект. Особено, когато обект на посегателство е интелектуалната собственост на предприятието, която е носител на неговия специфичен бизнес имидж. Оттук насетне значението на индустриалния контрашпионаж в предприятията за осведомеността от среда-

та и възможностите за ранно предупреждение трябва и ще продължава да се засилва.

Използвана литература

1. Бояджиев, Т. Изповед на шпионина. София: Сиела, 2018.
2. Василев, Е. Фирмена сигурност: Нелоялна конкуренция и фирмен контрашпионаж. София: Труд, 2000.
3. Закон за защита на конкуренцията: изм. ДВ. бр.7 от 19 Януари 2018 г. Достъпно на: http://www.lex.bg/bg/laws/ldoc/2135607845
4. Иванов, Ц. В. Модел на система за активна корпоративна сигурност в индустриалните предприятия в Република България. Дис. Варна, 2018.
5. Начев, Й. Конкурентно разузнаване. София: Сиела, 2007.
6. Полмър, Н. и Т.Б. Алън. Енциклопедия на шпионажа. София: Труд, 2001.
7. 18 U.S.Code §1839(3): https://www.law.cornell.edu/ uscode/text/18/1839
8. Allsopp, W. (2009) *Unauthorized Access: Physical Penetration Testing for IT Security Teams.* Wiley.
9. Bernhardt, D. (2003) *Competitive Intelligence: How to acquire and use corporate intelligence and counter-intelligence.* London: Pearson Education Ltd.
10. Burgess, Cr. & R. Power. (2008) *Secrets Stolen, Fortunes Lost: Preventing Intellectual Property Theft and Economic Espionage in the 21st Century*. Syngress Publishing.
11. Fink, S. (2002) *Sticky Fingers: Managing the Global Risk of Economic Espionage.* Chicago: Dearborn Trade Publishing.
12. Grooms, Th. F. (2016) *Market Intelligence… The Original Work.* CreateSpace Independent Publishing Platform, 1st Edition.
13. Mitnick, K. (2003) *The Art of Deception*. Wiley.
14. Nasheri, H. (2005) *Economic Espionage and Industrial Spying.* NY: Cambridge University Press.

15. National Counterintelligence and Security Center (2016) *National Counterintelligence Strategy of the United States of America 2016.* Washington DC: Office of the Director of National Intelligence.

16. National Counterintelligence and Security Center (2018) *Strategic Plan 2018-2022.* . Washington DC: Office of the Director of National Intelligence.

17. Walker, D. & Co. (2017) *Top Security Threats and Management Issues Facing Corporate America: 2016 Survey of Fortune 1000 Companies.* Parsippany, NJ: Securitas Security Services Inc.

18. Winkler, I. (1997) *Corporate Espionage.* Rocklin, CA: Prima Publishing.

19. U.S. Marine Corps (2007) *Counterintelligence.* NY: Cosimo Reports, Inc.

Контакти:
д-р Цанко Валентинов Иванов
E-mail: tsanko_ivanov@ue-varna.bg