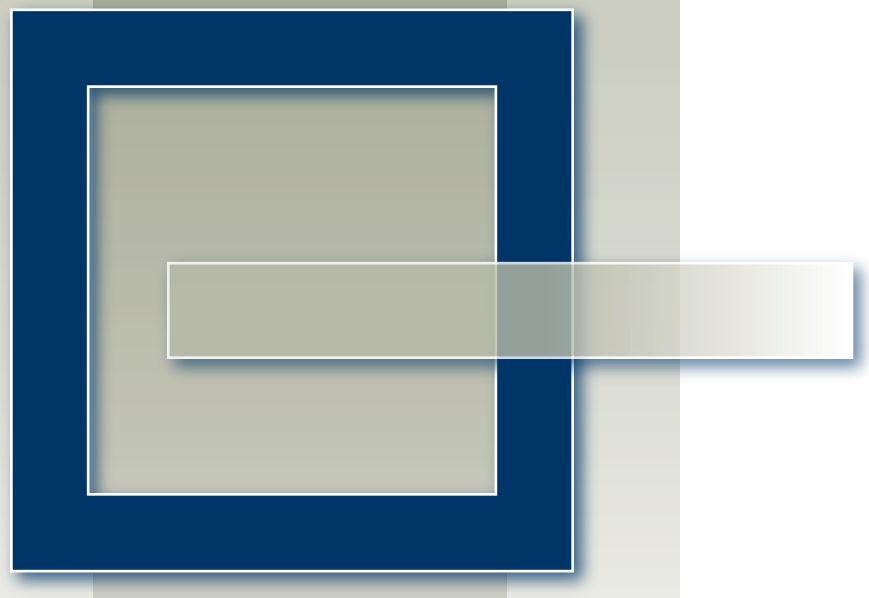


ДОБРИ ПРАКТИКИ ЗА БОРБА С КОРУПЦИЯТА И РАЗСЛЕДВАНЕТО НА ИЗМАМИ СЪС СРЕДСТВА ОТ ЕС

ДОБРИ ПРАКТИКИ ЗА БОРБА С КОРУПЦИЯТА И РАЗСЛЕДВАНЕТО НА ИЗМАМИ СЪС СРЕДСТВА ОТ ЕС

ЦЕНТЪР ЗА ИЗСЛЕДВАНЕ НА ДЕМОКРАЦИЯТА

Тази публикация е финансирана по програма „ХЕРКУЛЕС III" на Европейския съюз. Съдържанието на публикацията представя гледната точка на неговите автори, които единствени носят отговорност за него.
Европейската комисия не отговаряза начина, по който може да бъде използвана съдържащата се в него информация.

Настоящата публикация представя избрани добри практики и инструменти за разследване и предотвратяване на измами и корупционни практики при финансирането със средства от ЕС, като основната ѝ цел е да предостави на служителите от релевантните институции в България и в Румъния иновативни подходи за противодействие на тези престъпления в рамките на сложния многопластов национален механизъм за финансиране от ЕС.

За основа на публикацията служат темите, обсъдени по време на международната конференция „Заедно срещу завладяването на държавата: иновативни методи за разследване на измамите и корупцията с европейските средства за земеделие", проведена на 13-14 септември 2018 г. в София, с подкрепата на Европейската служба за борба с измамите (ОЛАФ).

ISBN: 978-954-477-356-4

ул. „Александър Жендов" 5, 1113 София
тел.: (+359 2) 971 3000, факс: (+359 2) 971 2233
www.csd.bg, csd@online.bg

СЪДЪРЖАНИЕ

СПИСЪК НА СЪКРАЩЕНИЯТА

ДФЕС	Договор за функциониране на Европейския съюз
ЕЗФРСР	Европейския земеделски фонд за развитие на селските райони
ЕФГЗ	Европейския фонд за гарантиране на земеделието
ОИСР	Организацията за икономическо сътрудничество и развитие
ОЛАФ	Европейската служба за борба с измамите
ОСП	общата селскостопанска политика
РСР	развитие на селските райони

СПИСЪК НА ФИГУРИТЕ

СПИСЪК НА КАРЕТАТА

УВОД

Европейският съюз (ЕС) провежда множество политики, които задълбочават интеграционния процес и имат общата цел да подобрят живота на гражданите му. За тези политики обаче, е необходим определен финансов ресурс, който се отделя от бюджета на ЕС чрез нетните вноски на държавите членки. Проблемът е, че пагубно влияние върху изпълнението на политиките, съответно върху отделяните средства за изпълнението им, оказват нарушения, умишлени или не, засягащи бюджета на ЕС, а именно извършените **нередности** и **измами** с европейски средства. С бюджет за плащания през 2018 г. в размер на **144,7 млрд. евро** и поети задължения в размер на **160,1 млрд. евро**[1], всяко едно засягане на отпусканите суми представлява сериозна вреда, която се заплаща от гражданите на ЕС.

За последните 50 години от създаването си, като една от най-важните политики за ЕС и неговите граждани, се е утвърдила общата селскостопанска политика (ОСП). Макар и през годините делът на финансиране на ОСП като процент от общия бюджет на ЕС да спада, то значимостта ѝ остава особено висока. Това е така, тъй като през 2018 г. в ЕС има над **510 млн.** потребители на земеделското производство, **12 млн.** от които са и самите фермери. Те обработват **48 % от площта на ЕС** и осигуряват 44 млн. работни места в рамките на хранителната верига, като около 113 млн. души живеят в селски райони[2]. Значимостта на ОСП е още по-висока за държави с традиционна селскостопанска ангажираност и необходимост от подобрения в земеделието, например: България, с площ 110 900 кв. км, 81 % от които представляват т.нар. селски райони, като от този процент 46,1 % са земеделски земи, а 37,4 % гори. Подобна е картината в Румъния, където 50 % от земята е земеделска, а 31 % е горска. За сравнение, в Белгия едва 14,5 % от земята е земеделска, а горите покриват 24 % от територията.

Показателен за важността на политиката е и фактът, че през 1985 г. 73 % от целия бюджет на Общността се е разходвал в рамките на ОСП. През 2016 г. и 2017 г. този процент спада до около 40 %[3], а през 2018 г. до около 38 %, като причина за този спад е реформата в ОСП и финансирането на други важни за гражданите политики. Независимо от спада, бюджетът на ОСП продължава да представлява почти половината от общия бюджет на ЕС. Общият бюджет на ОСП за периода 2014 – 2020 г. е в размер от **408 млрд. евро**[4].

---

1 https://www.consilium.europa.eu/en/press/press-releases/2017/11/30/2018-eu-budget-adopted/.

2 https://epthinktank.eu/2016/07/20/how-the-eu-budget-is-spent-common-agricultural-policy/.

3 https://ec.europa.eu/agriculture/sites/agriculture/files/cap-post-2013/graphs/graph1_en.pdf и Докладите по чл. 325 ДФЕС за 2016 г. и 2017 г.

4 http://www.europarl.europa.eu/factsheets/bg/sheet/106/%D1%84%D0%B8%D0%BD%D0%B0%D0%BD%D1%81%D0%B8%D1%80%D0%B0%D0%BD%D0%B5-%D0%BD%D0%B0-%D0%BE%D1%81%D0%BF.

От тези средства, **58,82 млрд. евро** са отпуснати през 2018 г. за помощ на фермерите, от които: **41,74 млрд.** евро за директни плащания, **14,37 млрд.** евро за мерки за развитие на селските райони и **2,7 млрд.** евро за пазарни мерки.

Финансирането на ОСП за сметка на общия бюджет се извършва чрез пряко финансиране или в контекста на споделеното управление с държавите членки и обхваща два основни компонента: **пряка помощ чрез преки плащания** към земеделските стопани и мерки за подкрепа на пазара, финансирани от Европейския фонд за гарантиране на земеделието (ЕФГЗ) – около 80 % от бюджета на ОСП; **и развитие на селските райони** (РСР), финансирано основно от Европейския земеделски фонд за развитие на селските райони (ЕЗФРСР) – останалите 20 % от бюджета на ОСП.

С оглед на обема на отпусканите средства, ОСП е подложена на **висок риск от измами**, поради което защитата на финансовите интереси на Европейския съюз е основен елемент както в управленския му ред, така и в дневния ред на държавите членки, които отговарят за управлението на над 70 % от средствата от европейските фондове. Затова чл. 325 от *Договора за функциониране на Европейския съюз* (ДФЕС) изисква ЕС и държавите членки да се борят с измамата и с всяка друга незаконна дейност, която засяга финансовите интереси на ЕС, като приемат мерки, които имат възпиращо действие и предлагат ефикасна защита в държавите членки, както и в институциите, органите, службите и агенциите на Съюза. Нещо повече, държавите следва като минимум да приемат същите мерки за борба с измамата, засягаща финансовите интереси на ЕС, каквито предприемат за борба с измамата, засягаща собствените им финансови интереси.

Тази активност обхваща т.нар. **цикъл за борба с измамите**, който включва **превенцията, откриването, разследването и санкционирането на измамите** и може да се извърши чрез най-широк набор от мерки, в т.ч. административни, наказателни, организационни и др. в рамките на действаща политика за борба с измамите – на европейско или национално ниво.

Настоящата компилация разглежда избрани най-добри практики, свързани със заплахата от измами и корупция, като основната ѝ цел е да предостави на ангажираните институции в България и в Румъния съвременни подходи за справяне с тези заплахи. Тя прави преглед и на разнообразни мултидисциплинарни теми и въпроси, обсъдени по време на международната конференция *„Заедно срещу завладяването на държавата: иновативни методи за разследване на измамите и корупцията с европейските средства за земеделие"*, проведена на 13-14 септември 2018 г. в София, с подкрепата на Европейската служба за борба с измамите (ОЛАФ). В публикацията са включени както традиционните и добре установени инструменти и методи за откриване и предотвратяване на корупционни практики при обществените поръчки, така и по-съвременни и иновативни способи, като например „сканиране на хоризонта", събиране на електронни доказа-

телства и работа с техники за разследване чрез отворени източници на информация.

Първата част на публикацията прави преглед на текущото състояние на практиките по предотвратяването и разследването на измами и случаи на корупция на равнище ЕС, с което подготвя по-ясна гледна точка за представянето на останалите части от ръководството В тази част са описани и действащата правна рамка, структурата и концепциите в контекста на цялостната схема на ЕС за борба с измамите и корупцията.

Част 2 представя методологическите аспекти за разкриване и предотвратяване на тези престъпления, като прави преглед на показателите за риска, приложими за измамите и корупцията. Разглеждането на съществуващите показатели за измами при възлагането на поръчки и въпросите за диагностициране на корупцията допълнително допринасят за разширяване на хоризонта на разследващите. Втората част завършва с преглед на картата на рисковете, която предлага изчерпателен списък на средствата/практиките, чрез които основните видове договори за обществени поръчки могат да бъдат опорочени с корупция или измами.

Част 3 прави обзор на по-иновативните, практични и перспективни инструменти, техники и подходи за предотвратяване и разследване на измами. Разузнаването от публични и открити източници на информация – OSINT, като например такива в интернет пространството (вкл. социалните мрежи), може да има решаващо значение за насочването на усилията при разследване и за потвърждаването на изводи и предположения. В същото време, ефективното осигуряване на цифрови/електронни доказателства се превръща във все по-решаващ фактор за съдебната фаза, тъй като във все по-голяма степен сделките и документите се създават, разпространяват и съхраняват по електронен път. От друга страна, инструментите за прогнозна оценка, като например „сканиране на хоризонта", се смятат за изключително полезни за предотвратяването на измами, тъй като те са насочени към идентифициране на бъдещи заплахи и предизвикателства, свързани с потенциални и вероятни подходи за осъществяване на измами. Особено като се има предвид бързият технологичен напредък, „сканирането на хоризонта" може да донесе много ценна информация за бъдещите нужди по предотвратяването на измами.

ЧАСТ 1. КОНТЕКСТ

Европейската служба за борба с измамите – ОЛАФ е служба в рамките на Европейската комисия със статут на Генерална дирекция, създадена през 1999 г., която разполага с правото да извършва независими **административни разследвания** с цел борба срещу измамите, корупцията и всяка друга незаконна дейност, засягаща финансовите интереси на Съюза. Това означава, че нито една друга институция, орган, служба или агенция на ЕС няма право да се меси в рамките на провеждането на разследвания, а до стартиране на функционирането на Европейската прокуратура, ОЛАФ остава единственият орган, който има мандат да извършва разследвания на европейско ниво за защита на финансовите интереси на ЕС.

Разследванията на ОЛАФ биват два вида: **външни разследвания**, които обхващат всички разходи на Европейския съюз, с акцент върху Европейските структурни и инвестиционни фондове (ЕСИФ) и селскостопанската политика; преките разходи и външната помощ, както и някои приходи на ЕС, и **вътрешни разследвания** – които се отнасят до законосъобразното изпълнение на задълженията на служители и членове на институциите на ЕС. Поради тази причина, ролята на ОЛАФ може да бъде обобщена в две направления:

- да извършва разследвания за защита на финансовите интереси на ЕС;
- да развива политиката за борба с измамите.

Фигура 1 представя най-активните области на разследване от страна на ОЛАФ по критерий – **водени разследвания**[5] към 2017 г. Най-активните области в рамките на водените през 2017 г. разследвания са: структурните фондове, **земеделските фондове**, директните плащания и външната помощ, най-малко разследвания са водени по отношение на разходите в социалния фонд, новите финансови инструменти и тютюневите изделия и фалшифицираните стоки. Това означава, че водените разследвания в областта на земеделието[6] представляват 12,7 % от всички открити разследвания през 2014 г.; 9 % през 2015 г., 6,1 % през 2016 г. и 6 % през 2017 г. Статистическата тенденция за намаляване на водените разследвания в областта на земеделието не означава аналогичен спад в броя на нередностите и измамите в същата област, поради което предприемането на мерки за борба с измамите в областта на земеделието следва да остане приоритет на европейския и националния дневен ред.

Наказателните разследванията на ниво ЕС са възложени на **Европейската прокуратура,** която отговаря за провеждането на разслед-

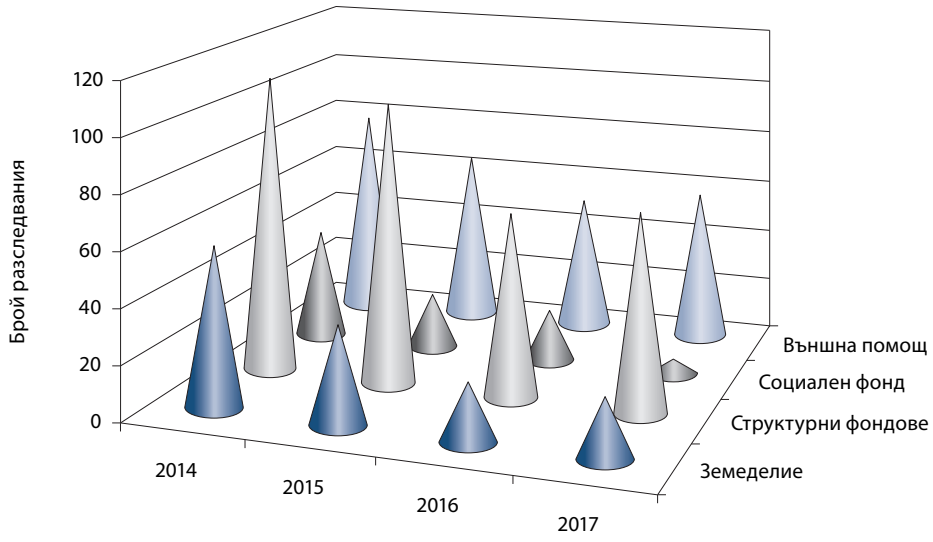
---

[5] По информация на годишния доклад на ОЛАФ за 2017 г.

[6] Общият брой открити разследвания за 2014 г. е 474, за 2015 г. – 398, за 2016 г. – 344.

вания, наказателното преследване и предаването на съд на извършителите на престъпления и съучастниците в престъпления, засягащи финансовите интереси на Съюза, които са предвидени в Директива 2017/1371 относно борбата с измамите, засягащи финансовите интереси на Съюза по наказателноправен ред (PIF Директивата). Функционирането на Европейската прокуратура ще **промени облика** на борбата с измамите, тъй като до влизането в сила на Регламент 2017/1939 само органите в държавите членки могат да водят наказателни разследвания на измами и да повдигат обвинения по случаи със средства от ЕС, и то при териториална и функционално ограничена компетентност[7]. След стартиране работата на Европейската прокуратура, тя ще провежда разследвания и ще осъществява наказателно преследване, както и ще упражнява обвинителна функция пред компетентните съдилища на държавите членки до окончателното приключване на делото.

Фигура 1. Водени от ОЛАФ разследвания към 2017 г. в областта на земеделието за периода 2014 – 2017 г., съпоставени с други области на разследване



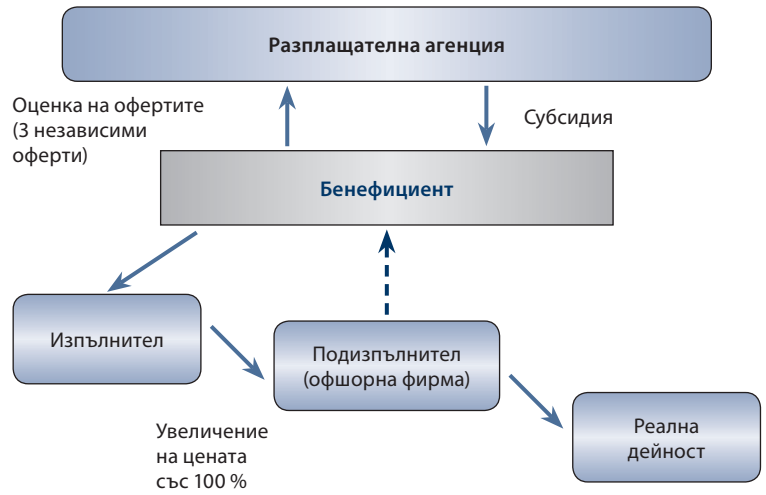
	2014	2015	2016	2017
Земеделие	60	36	21	22
Структурни фондове	111	104	69	73
Социален фонд	42	21	19	5
Външна помощ	79	66	52	58

Източник: *По информация на годишния доклад на ОЛАФ за 2017 г.*

[7] ЕК, ОЛАФ, Евроджъст и Европол нямат мандат да водят наказателни разследвания.

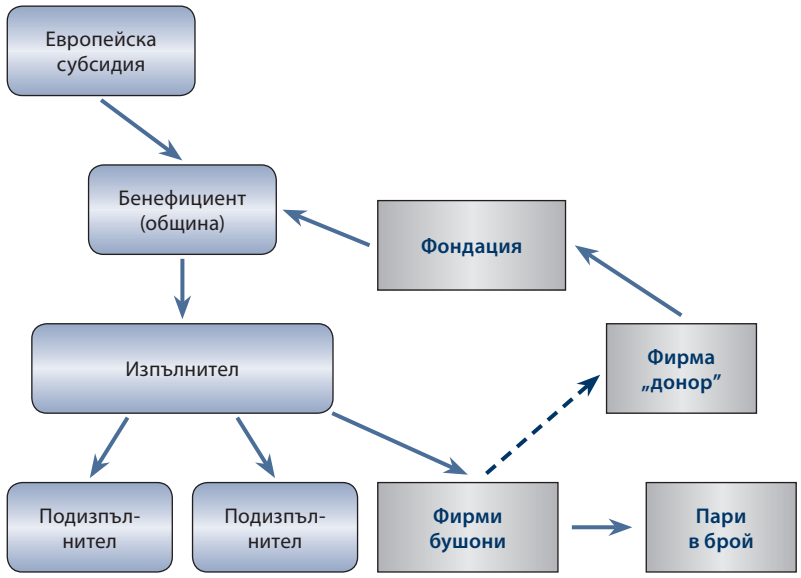
Най-често срещаните специфични начини на действие

Фигура 2. Примерна схема за измама с Европейски средства за земеделие



Източник: *На база презентации по време на Конференцията.*

Фигура 3. Финансови потоци в схема за измами с Европейско финансиране



Източник: *На база презентации по време на Конференцията.*

Най-често срещаните специфични начини на действие (типове ***modus operandi)*** в измамите в земеделието за периода 2013 – 2017 г. включват фалшиви или фалшифицирани документи, както и фалшиви или фалшифицирани искания за плащания. Наблюдават се и **множество други начини за извършване на измама**: надсмятане, наддекларирание на численост на лимити и квоти, конфликт на интереси, подкуп и други корупционни действия, създаване на изкуствени условия[8], подправени спецификации, изтичане на информация за офертите, разбиване на обществени поръчки, подмяна на стоки и др.

Типични примери за злоупотреби, установени в рамките на разследванията, са: закупуване на техника втора ръка и субсидирането ѝ като нова; злоупотребяване с правилото за трите оферти; субсидиране на къща за гости, която се използва за личен дом; заобикаляне на максималния размер на помощта (напр. майка и две дъщери кандидатстват поотделно и после построяват общ обект); разделяне на търговската насоченост на дружество в две нови дружества, за да може да се кандидатства в две различни направления; субсидиране за определен брой култури или животни, които не са налични или са посочени неверни видове за получаване на по-голяма субсидия (напр. по-рядка порода коне) и др. Различните начини за извършване на измама обу-

[8] Доклад на ЕК по чл. 325 ДФЕС за 2017 г., т. 3.3.

славят необходимост от специфични знания на проверяващите органи, тъй като сложността на измамата често е правопропорционална на обема на засегнатите средства.

Иновативни методи за борба с измамите

За да се отговори на предизвикателствата в областта на ОСП е необходимо нормотворчеството и функционирането на институциите в областта на разследванията да бъдат все по-актуални. Борбата с измамите е пряко зависима от начина, по който нарушенията или престъпленията се извършват, техният ***modus operandi***. Прието е да се счита, че лицата, които извършват измами, са винаги една крачка пред отговорните институции, а установеният подход в исторически контекст за борба с измамите следва формулата: **извършителство → разследване → опит за възстановяване на средства.** Профилирането[9] на измамниците е един от методите за типологизиране на начините, по които действат измамниците, а оттам – и на предприемане на единни мерки и въвеждане на стандарти при борбата с измамите. Важно е да се посочи, че институциите в Европейския съюз и държавите членки могат да дефинират и предприемат иновативни мерки за борба с измамите с цел в бъдеще **институциите да бъдат една крачка пред евентуалните извършители** или да бъде възможна т.нар. **перфектна превенция.** На практика държавите членки са длъжни да предприемат минимум същия набор от мерки за защита на европейския бюджет, какъвто е установен за националния, давайки свободата националните мерки да бъдат още по-нови, с още по-голяма добавена стойност и най-вече иновативност, изпреварваща тази на измамниците.

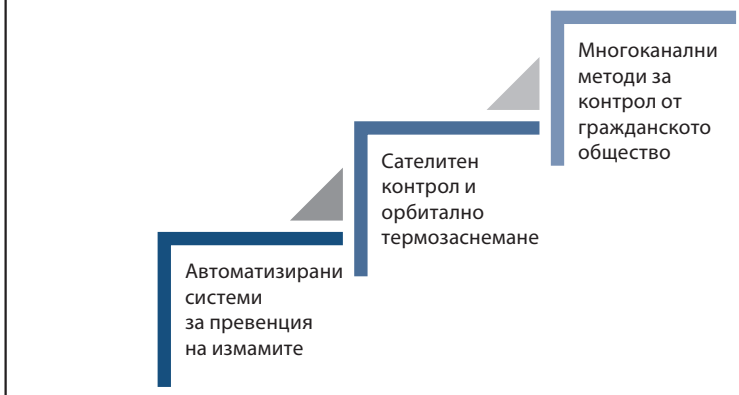
Поради тази причина, следва да бъде обърнато специално внимание на мерките, които държавите членки биха могли да въведат в борбата с измамите и по-добра защита на селскостопанската политика чрез въвеждането или използването на възможностите на т.нар. **иновативни методи за борба с измамите в земеделието**, обобщени в три категории в рамките на настоящото изследване:

1. **Автоматизирани системи за докладване на съмнителни обстоятелства** – с развиването на IT технологиите и AI – изкуствения интелект, въвеждането на електронен контрол и автоматизирани системи, които да идентифицират червени флагчета и потенциално рискови ситуации и конфликт на интереси би имало сериозна добавена стойност и високо ниво на превенция. За осъществяването на такава мярка биха могли да се използват настоящи действащи превантивни системи (напр. EDES), бази данни в областта на земеделието (напр. IACS) и борбата с измамите (напр. IMS), възможности за *data mining*[10], имащи за цел идентифициране на незаконни (корупционни, измамни и др.) модели на поведение. Добър пример за сходна система е *"Prevent"* на Агенцията за интегритета в Румъния, представляваща компютъризирана система, която идентифицира и

[9] https://www.oreilly.com/library/view/profiling-the-fraudster/9781118929766/.

[10] Англ. събиране и обработка на информация.

Фигура 4. Иновативни методи за борба с измамите



не позволява възникването на конфликт на интереси в реално време в областта на обществените поръчки с европейски средства[11]. Важно внимание и евентуално инкорпориране на информацията в рамките на автоматизираните системи за докладване биха представлявали и извършваните от разследващите органи дигитални криминалистични операции[12].

2. **Сателитен контрол[13] и орбитално термозаснемане –** и към настоящия момент се използват възможностите на орбиталната технология, вкл. сателитното заснемане на времеви условия и площи, напр. системата на сателитите по програма „Коперник". Разширяването на достъпа до такава технология и до разследващите органи, вкл. с хронологична функция за връщане на термални и заснемания на площи, би позволила установяване на обективно фактическо състояние. Често при извършването на проверка, одит или разследване в областта на земеделието възниква проблемът, че твърдяното нарушение (използване на непозволени препарати, определен вид продукция, обем на продукцията и т.н.), което се е случило през топлата част на годината, следва да бъде проверено месеци след това, когато на практика вече няма как обективно да бъдат установени тези факти.
3. **Иновативни многоканални методи за контрол от гражданското общество –** в рамките на този метод е заложен принципът на контрол от страна на гражданите на ЕС и създаването на национално самосъзнание, свързано с **нулева толерантност към измамите**. Това би могло да стане по различни начини:
   - чрез социални кампании и използване на информационен метадата маркер – т.нар. хаштаг. Пример за социална кампания, целяща нулева толерантност на обществото, е **FraudOff!** кампа-

[11] https://www.uti.eu.com/business-lines/information-technology-and-communications/smart-government-solutions/portfolio/prevent-national-integrity-agency-ani/.

[12] Такива действия се извършват от ОЛАФ, АФКОС и разследващи органи и имат за цел осигуряване на доказателствен материал от дигитални образи (документи, снимки, файлове, кореспонденция и др).

[13] В.ж. чл. 26 „придобиване на сателитни изображения" от Регламент 908/2014 в областта на земеделието https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014R0908.

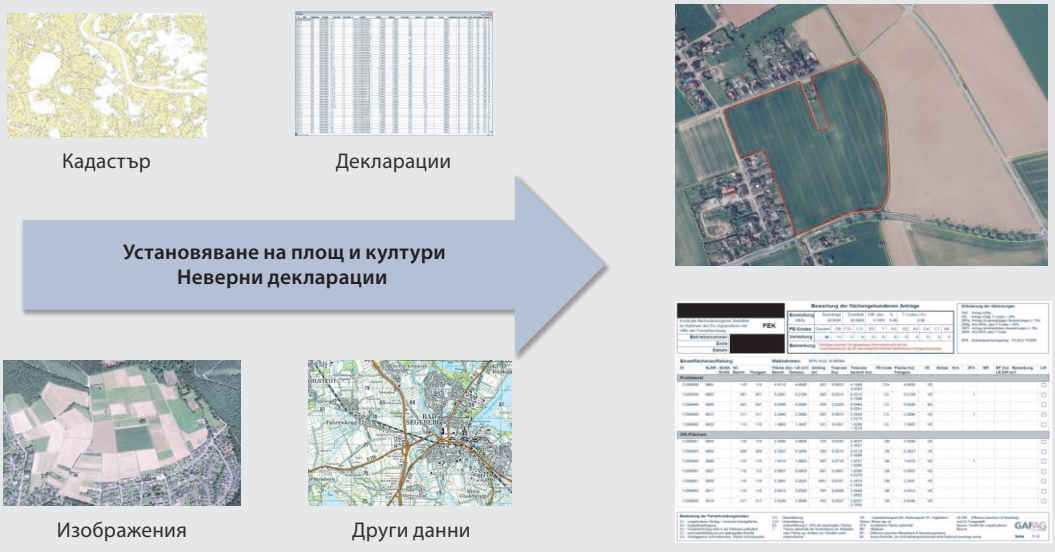
нията на властите в Латвия, която обединява повече от 20 държавни институции и частни партньори под хаштага #Fraudoff, което прави всеки един сигнал или информация достъпен в социалните мрежи едновременно за всички участници.

- Чрез въвеждане на поощрителни обучителни мероприятия за подрастващи. Република Малта има опит във въвеждане на поощрителна образователна кампания в средните училища. Предлага се кратък тест от 10 въпроса, свързани с борбата с измамите, като правилно отговорилите ученици участват в томбола за предметна награда.

Каре 1. Използване на технологии за дистанционно наблюдение за предотвратяване и разкриване на измами

Новите правила, влезли в сила на 22 май 2018 г., ще позволят използване на данните от сателитите "Sentinel" по програма „Коперник" на ЕС и на други данни от наблюдения на Земята като доказателства при проверка на изпълнението от страна на земеделските стопани на изискванията на ОСП за плащания въз основа на площ (директни плащания към земеделски стопани. Същите ще могат да се използват и при плащания за подпомагане на развитието на селските райони, както и на изискванията за кръстосано съответствие, като например тези относно горенето на стърнищата.

Прилагането на технологии за дистанционно наблюдение и ГИС служи като обективна методика за осъществяване на задължителния административен контрол върху допустимостта на декларациите за субсидиране. Проверката на декларираните култури, съответните площи в LPIS и конкретното съдържание на декларациите се осъществява въз основа на геопространствени бази данни, включително LPIS, DOP, VHR и HR данни, както и интегрираната административна процедура за контрол. Този ефикасен подход е от полза и при традиционните проверки на място, тъй като той намалява времето и разходите за тяхното осъществяване и предлага обективни, приемливи и надеждни резултати.



Източник: *На база презентации по време на Конференцията.*

- Чрез създаване на централизирано приложение за борба с измамите в пазарите за приложения на системите Android и iOS, в рамките на което да се получава информация с QR код за всеки проект, както и да се подава сигнал за нередност и измама със снимков, аудио или видео материал.
- Чрез развитие на разследваща журналистика[14].

[14] Напр. "Rise Project" в Румъния https://www.riseproject.ro/ или „Биволъ" в България https://bivol.bg/.

ЧАСТ 2. ДОБРИ ПРАКТИКИ

ИДЕНТИФИЦИРАНЕ НА РИСКОВЕТЕ ОТ КОРУПЦИЯ ПРИ ПРОЦЕДУРИТЕ ЗА ВЪЗЛАГАНЕ НА ОБЩЕСТВЕНИ ПОРЪЧКИ[15]

Обществените поръчки са сред сферите на управлението на публичния сектор, отличаващи се с най-висок риск от корупция и злоупотреби. Независимо от многообразието на форми, всички злоупотреби в тази сфера имат една обща цел – насочване на финансов ресурс от разпоредителите с бюджетни средства, както и от държавните и общинските предприятия, към предварително определен победител с цел лично облагодетелстване[16]. Събирайки голям брой заинтересовани страни на пазар на стойност милиарди евро годишно, системата на обществените поръчки е сред най-уязвимите дейности на публичната власт. Корупционните действия и измамните практики в тази област ощетяват интереса на гражданите както в развитите, така и в развиващите се държави.

Въпреки съществуващите контролни механизми, при много от обществените поръчки се допускат грешки, нередности, измами и други злоупотреби с обществени фондове. Повечето от грешките и нередностите могат да бъдат обяснени с недостатъчна информираност на част от участващите в тях лица и структури – доставчици, счетоводители, одитори и др. Подобни отклонения могат да бъдат преодолени с помощта на допълнителна подготовка. За разлика от тях, измамите и корупцията са по-трудни за идентифициране, тъй като са резултат от преднамерени усилия за заобикаляне на правилата с оглед получаването на неследващи се облаги, както и за прикриване следите на извършителите.

В контекста на такъв многопластов проблем, настоящият практически наръчник представя преглед на добрите практики, които могат да се използват при противодействие на заплахите от измами и злоупотреби в процеса на обществените поръчки. Сложните процеси на злоупотреби и различните типове измамни практики в отделните фази на обществените поръчки са разгледани последователно, чрез анализ на основните компоненти и преглед на международно признати подходи за противодействие на рисковете от корупция и измами. Специфичен фокус е поставен и върху конкретиката, проблемите и предизвикателствата на българския пазар и система на обществени поръчки (ОП).

---

[15] За основа служи документът: Престъпност при обществените поръчки: Практическо ръководство за предотвратяване, противодействие и анализ на рисковете от корупция, Център за изследване на демокрацията, 2016.

[16] Център за изследване на демокрацията. Корупцията при обществените поръчки: рискове и противодействие. София, 2006.

Разгледани са международно признатите **Принципи за укрепване на интегритета при обществените поръчки**[17], разработени от Организацията за икономическо сътрудничество и развитие (ОИСР). В допълнение на принципите, ОИСР прави задълбочен преглед на типовете измамни практики във всеки един етап от възлагането и изпълнението на обществените поръчки – предтръжна, тръжна и следтръжна фаза – чрез анализ на начините, използвани за отклоняване на държавни средства, както и различните видове измами. Индикаторите за риск насочват вниманието към ключовите аспекти при възлагането на обществени поръчки, които трябва да бъдат контролирани. Затова, след типовете измамни практики и рисковете във всеки един етап от възлагането и изпълнението на обществените поръчки, са разгледани **индикаторите за наличие на рискове**.

Представени са методите за измерване на ефективността от прилагането на различните подходи и мерки за намаляване нивото на злоупотреби и корупция в процеса на обществените поръчки. По-конкретно са разгледани три методики за измерване на злоупотребите и измамите при обществените поръчки.

ПРИНЦИПИ ЗА УКРЕПВАНЕ НА ИНТЕГРИТЕТА ПРИ ОБЩЕСТВЕНИТЕ ПОРЪЧКИ[18]

Принципите за укрепване на интегритета при обществените поръчки служат като общо ръководство на правителствата при подготовката и внедряването на ефективна рамка за възлагане и изпълнение на обществени поръчки, като в същото време се вземат под внимание отделните нормативни уредби и организационни структури на страните членки. Принципите са насочени основно към държавни служители на национално ниво, определящи политиката в областта на обществените поръчки, но биха могли да се ползват и на ниво регионални власти, както и от мениджъри в държавните предприятия. **Главната цел на принципите** е да направляват представителите на централната власт в утвърждаване културата на интегритет в цялата система на обществените поръчки, от оценката на публичните нужди до управлението на договорите и плащанията.

Определение за интегритет

Интегритетът може да бъде дефиниран като **използването на фондове, ресурси, власт и други активи според официално заявените цели и в съответствие с обществения интерес**. Един „негативен" подход за дефиниране на интегритета също би бил полезен при определянето на по-ефективна стратегия за предотвратяване на на-

[17] Организация за икономическо сътрудничество и развитие (ОИСР). Принципи за укрепване на интегритета при обществените поръчки. Париж: OECD Publishing, 2009.

[18] Организация за икономическо сътрудничество и развитие (ОИСР). Принципи за укрепване на интегритета при обществените поръчки [OECD Principles for Integrity in Public Procurement]. Париж: OECD Publishing, 2009.

рушенията в обществените поръчки. Тези нарушения на интегритета включват:

- корупция, в т.ч. подкупи, „рушвети", използване на роднински и приятелски връзки и клиентелизъм;
- измама и кражба на ресурси, като подмяна на стоки, което води до по-нискокачествени продукти;
- конфликт на интереси в обществените услуги и при получаването на работа след приключване на мандат в публичния сектор;
- тайни договорки и съглашения;
- злоупотреба и манипулиране на информация, включително търговия с влияние;
- дискриминационно отношение в процеса на обществените поръчки;
- прахосничество и злоупотреба с ресурси на организацията.

Основни „стълбове" на принципите за укрепване на интегритета в обществените поръчки

Принципите наблягат върху значението на процедурите за засилване на прозрачността, доброто управление, превенцията на нарушения, както и отчетността и контрола при обществените поръчки.

A. Прозрачност

1. *Осигуряване на достатъчно ниво на прозрачност в цялата система на обществените поръчки, за да се гарантира честно и справедливо третиране на потенциалните доставчици.*
2. *Максимизиране на прозрачността в конкурентните тръжни процедури и вземане на предпазни мерки за засилване на интегритета, особено в случаите, когато се допуска изключение от конкурентна процедура.*

B. Добро управление

1. *Гаранции, че обществените фондове се използват в обществените поръчки според определените цели.*
2. *Гаранции, че официалните лица в обществените поръчки отговарят на високи професионални стандарти за знания, умения и интегритет.*

C. Превенция на евентуални нарушения; спазване на регламентите; мониторинг

1. *Използването на механизми за предотвратяване на рисковете за интегритета в обществените поръчки.*
2. *Насърчаване на тясно сътрудничество между правителството и частния сектор за поддържане на високите стандарти за интегритет, особено в управлението на договорите.*
3. *Осигуряване на специфични механизми за мониторинг на обществените поръчки, както и за установяване на нарушенията и налагане на съответните санкции.*

Каре 2. Най-добри практики за предотвратяване на конфликт на интереси, Национална агенция за интегритет, Румъния

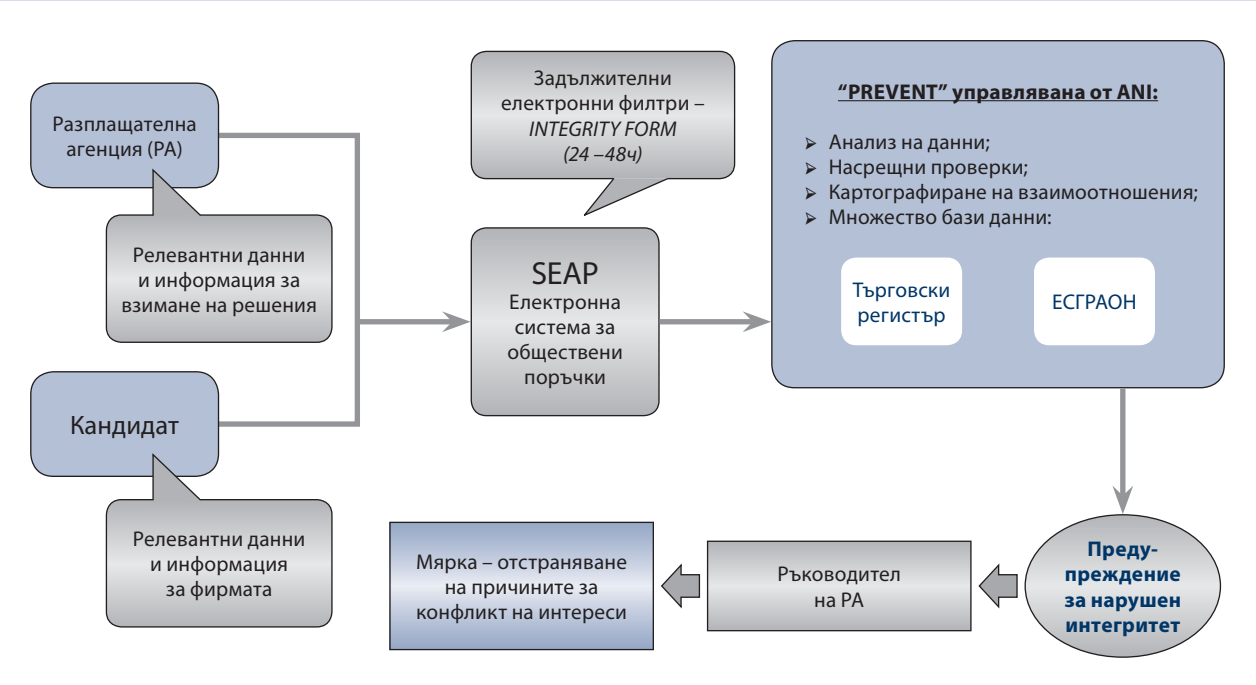
PREVENT представлява интегрирана компютърна система, предназначена за предотвратяване на конфликти на интереси, в реално време. Проектът е разработен от Румънската национална агенция за интегритет (ANI) и в първата си фаза системата идентифицира случаи в областта на обществените поръчки с финансиране от ЕС; като впоследствие ще бъде разширена, за да обхване и националните обществени поръчки. Платформата е проектирана така, че да си взаимодейства със SEAP (Електронна система за обществени поръчки).

КОМПОНЕНТИ НА СИСТЕМАТА

Хардуер, COTS оборудване и софтуер | Комуникационна инфраструктура | Системна взаимосвързаност със SEAP | Интеграция в информационната система на Националната агенция за интегритет

ПОЛЗИ

Оптимизиране на вътрешните дейности на инспекторите по интегритета | Мониторинг на всички публични придобивания на национално равнище | Предотвратяване на конфликти на интереси, свързани с публичните придобивания в Румъния | Осигуряване на подходящи хардуерни и софтуерни технологии за получаване, съхранение, анализ и докладване на данни.



Източник: *На база презентации по време на Конференцията.*

Отчетност и контрол

1. *Изграждане на ясна система от отговорности, заедно с ефективни механизми за контрол.*
2. *Разглеждане на постъпили оплаквания от потенциални изпълнители по справедлив начин и в срок.*
3. *Овластяване на гражданските организации, медиите и широката общественост за критичен преглед на обществените поръчки.*

Прилагане на принципите – укрепване на интегритета във всеки един етап на цикъла на обществените поръчки – списък с мерки[19]

Списъкът с мерки представлява практически инструмент за прилагане на нормативната рамка за укрепване на интегритета във всеки един етап от цикъла на обществените поръчки, от оценката на публичните нужди до управлението на договорите и плащанията. Цикълът на обществените поръчки обхваща три основни фази:

- предтръжна процедура, включваща оценка на нуждите, планиране и бюджет, определяне на изискванията и избор на процедурите;
- тръжна процедура, включително публична покана за провеждането на търг, оценяване и възлагане на поръчката;
- следтръжна процедура, включваща управлението на договорите и плащането.

Списъкът съдържа конкретни процеси и мерки, с които длъжностните лица определят или доразвиват интегритета в цикъла на обществените поръчки. Правителствата трябва да гарантират, че тези мерки са подкрепени от необходимите правни, институционални и политически условия в страната.

1. Предтръжна фаза

   Рискове за интегритета в предварителната тръжна процедура – Предпазни мерки при предтръжната процедура

   - Етап 1. Оценка на нуждите
   - Етап 2. Планиране и бюджет
   - Етап 3. Определяне на изискванията
   - Етап 4. Избор на процедури

2. Тръжна фаза

   Рискове за интегритета в тръжната процедура – Предпазни мерки при тръжната процедура

   - Етап 5. Публична покана за участие в търг
   - Етап 6. Оценяване
   - Етап 7. Възлагане

[19] Организация за икономическо сътрудничество и развитие (ОИСР). Принципи за укрепване на интегритета при обществените поръчки. Париж: OECD Publishing, 2009.

Каре 3. Пример за злоупотреба с власт при схемите за финансиране на ЕС, APIA (Агенция за плащания и интервенции в земеделието), Румъния

Директорът на местен клон на APIA и негови съучастници периодично искат пари от бенефициент по програми на ЕС, в замяна на пренебрегване на несъответствия при мониторинга на субсидиите, одобрени за земеделските дейности на потърпевшите. Директорът на местния клон на APIA поискал €2 500 от земеделски стопанин, който имал няколко земеделски дейности, подлежащи на мониторинг от APIA. След като той платил първоначално исканата сума, директорът поискал още €5 000, за да продължи да пренебрегва нарушенията на потърпевшите, а след това и още €3 000. След третото искане, бенефициентът съобщил за случая и директорът от APIA бил заловен на местопрестъплението.

Източник: *На база презентации по време на Конференцията.*

3. Следтръжна фаза

Рискове за интегритета след възлагането – Предпазни мерки след приключване на тръжната процедура

- Етап 8. Управление на договорите
- Етап 9. Поръчка и плащане

ИЗГОТВЯНЕ НА КАРТА НА РИСКА – ИДЕНТИФИЦИРАНЕ НА РИСКОВЕТЕ ОТ ИЗМАМИ И КОРУПЦИЯ В ОБЩЕСТВЕНИТЕ ПОРЪЧКИ[20]

Обществените поръчки са особено уязвим за измами и корупция сектор. Затова са важни техниките за разкриване и превенция, които могат да ограничат злоупотребите. В настоящата глава са анализирани начините, използвани за отклоняване на държавни средства, както и различните видове измами. Този подход позволява на заинтересованите лица (държавни служители в този сектор, титуляри на изборни длъжности, бизнесмени, следователи, прокурори и др.) да оценят рисковете от измами и корупция.

Примерите са взети от практиката на страните – членки на Европейския съюз (ЕС) за дълъг период от време. Това позволява да бъде направен изводът, че измами са възможни и в държави със солидна и добре развита законова рамка, в които съществуват контролни инструменти, упражнявани от служители с доказана добросъвестност. Дори службите на Европейския съюз не са напълно защитени.

[20] Организация за икономическо сътрудничество и развитие (ОИСР). Принципи за интегритет при обществените поръчки. Управление на риска: разбиране на рисковете от измами и корупция в цикъла на обществените поръчки. Париж: OECD Publishing, 2009.

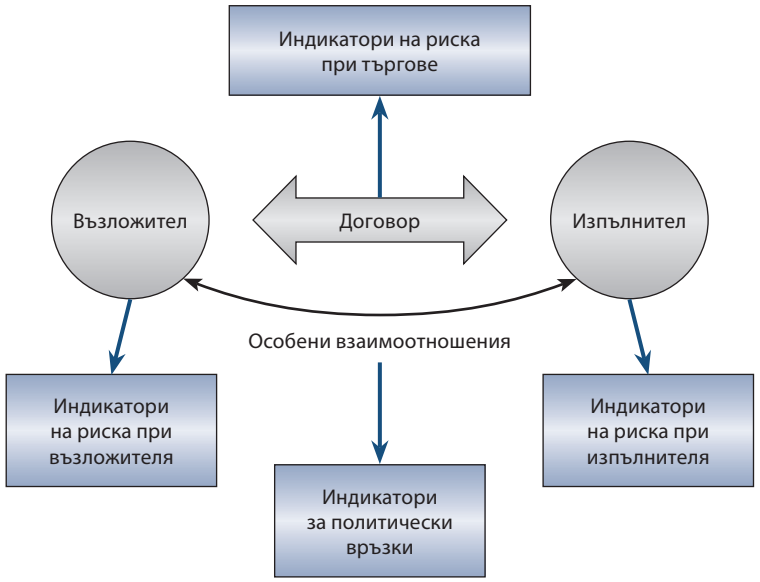
Каре 4. Пример за злоупотреба с власт, APIA (Агенция за плащания и интервенции в земеделието), Румъния

Извършителите (кмет, директор от APIA и служител в APIA) искали големи суми от земеделските стопани, като ги заплашвали, че ще им прекратят договорите за ползване на пасища. Потърпевшите получавали субсидии от ЕС под формата на преки плащания за пасища, отдадени за ползване от кметството. Един от земеделските стопани отказал да плати поисканата от кмета и длъжностните лица от APIA сума. Той подал сигнал в полицията и един от служителите на APIA бил заловен на местопрестъплението при получаване на 600 румънски леи (€150) от земеделския стопанин, представляващи част от поисканата сума.

Източник: *На база презентации по време на Конференцията.*

Въпреки съществуващите контролни механизми, за редица договори за обществени поръчки са характерни грешки, нередности, измами и други злоупотреби с обществени фондове или корупция. Повечето от тях могат да бъдат обяснени с недостатъчната информираност на част от участващите в тях лица и структури – доставчици, счетоводители, одитори и др. Подобни отклонения могат да бъдат преодолени с помощта на допълнителна подготовка. За разлика от тях, злоупотребите под формата на измами и корупция са по-трудни за идентифицирани, тъй като са резултат от преднамерени усилия за заобикаляне на правилата с оглед получаването на неследващи се облаги, както и за прикриване следите на извършителите.

Фигура 5. Пример за концептуализация на показателите за риска при обществените поръчки



Източник: *Fazekas, M., Cingolani, L., & Tóth, B. Цялостен преглед на обективни корупционни пълномощници при обществените поръчки: рискови участници, транзакции и средства за извличане на наеми: GTI-WP/2016:03. Будапеща: Институт за прозрачност на правителството, 2016.*

Затова е необходимо да се познават:

- Методите, които се използват на различните стадии на осъществяването на договорите за държавни поръчки и целят заблуждаването на външни наблюдатели и одитори, че измамните транзакции са законни.
- Техниките за злоупотреба със заделени по съответна сделка средства за тяхното използване (за лична облага или за друга цел), както и мрежите, чието използване позволява извършването на измамите.

При описанието на тези механизми е полезно да се разграничават рисковете от измама от тези от корупция: 1) при оценката на необходимите ресурси; 2) на равнище „планиране"; 3) при избирането на метода за селектиране и 4) при изпълнението на договора.

Рисковете при оценка на разходите

Дори на стадия, предшестващ подписването на договора, съществуват редица различни начини за злоупотреба с обществени средства под формата на възлагане на обзорни проучвания, неспазване на сроковете, необосновано увеличаване на цените и др. Въпросните злоупотреби често са по-малко от тези на стадия на изпълнението на контракта, но пък са по-лесни за прикриване. Сред тях е и увеличаването броя на плащанията, тъй като тази форма на злоупотреба може да бъде използвана на всеки етап от процеса на планиране на договора.

Каквото и да е предназначението на обзорното проучване, механизмът за незаконно отклоняване на средства си остава един и същ. Същевременно процедурите могат да приемат различна форма в зависимост от полезния ефект на предлаганото проучване. Ако целта е да се провери определена хипотеза, да се избере определен вариант или да се улесни вземането на определено решение, проучването следва да бъде задълбочено и да бъде направено от компетентна консултантска фирма. Обратното – ако не се преследва реална цел (например, когато съществува цялостна яснота за параметрите на проекта), проучването може да бъде възложено на всяка фирма, която се ограничава с ангажимента да предостави нужния документ, без да се задълбочава по случая. В някои случаи такава фирма не извършва никаква дейност, а просто се използва да инкасира договорената сума. С други думи, проучвателните документи могат да бъдат с високо качество или напълно незначителни. Очевидно ще бъде лесно да се открие злоупотреба, ако подобни проучвания са безполезни или с ниско качество, както и в случаите, когато въобще не се представят на клиента. Същевременно не винаги съществува корелация между качеството на проучването и отклонените средства: добри като качество проучвания могат да прикриват големи злоупотреби, докато некачествени проучвания могат да бъдат извършвани при спазване на правилата. Затова преди всичко е необходимо да се оцени за каква сума става въпрос, а след това отблизо да се контролира изразходването на паричните средства.

Малки проучвания

Тази категория обхваща всички проучвания, чиято стойност е под определения от националния регулатор праг. При тях служителят обикновено има право на избор на съответна фирма, без при това да обосновава своето предпочитание, тъй като обикновено е нужен само ваучер или разпореждане, за да получи нужната сума. Предоставянето на фактура е достатъчно за изплащане на сумата, при положение, че тя съответства на тази в разпореждането. Конвенционалният контрол в случая едва ли би могъл да открие каквато и да е злоупотреба.

Има няколко начина, чрез които длъжностното лице може да „отклони" пари за себе си, за свои близки или роднини, или за групата, с която е свързано. Но за подобна операция въпросното лице все пак ще се нуждае от помощта на консултант. Преди всичко парите могат да напуснат местната служба/държавно учреждение, като следват „легалните" канали, преди да бъдат „пренасочени" към избрания реципиент с помощта на посочените по-горе техники:

- „Приятелски" консултации. Длъжностното лице може да се свърже с „приятелски" тип консултант или организация, за да възложи извършването на работата. Това е процедура, която се използва често от някои политически партии при събиране на нужните им фондове. При използването на такива „приятелски" консултантски фирми отпада проблемът с конкуренцията. Избраната фирма може да получи хонорар, който е твърде голям за оказаната услуга (процесът се нарича *overbilling*). Той се формира от заплащането на реалната цена на проучването (каквото и да е неговото качество) плюс сумата, която длъжностното лице/разпоредителят реши да си присвои.
- Използване на юридическо лице, което е собственост на въпросния разпоредител. Последният може да възложи на своето юридическо лице или на членове на семейството си да извършат проучването.

Дублиране на проучвания

Длъжностното лице/възложителят също така може да поръча изготвянето на проучване едновременно или последователно на повече фирми. В случай че представят докладите си едновременно, тези фирми могат да бъдат накарани да работят заедно и да формират „картел". Техните хонорари ще бъдат „хармонизирани" така, че да гарантират най-голяма печалба. Обединени в подобен картел, фирмите си поделят договорите, а в някои случаи възлагат части от доклада на подизпълнители – техни колеги или конкуренти. Подобно „разделение на труда" е изгодно за всичките участници, включително и за възложителя, който ще си получи печалбата, която е заявил пред съответния консултант, който не е участвал в процеса на селекция. Ако разпоредителят разреши на изпълнителите да представят докладите си на различни дати, последната фирма, която ще представи своите резултати, може да се възползва от тези на предшествениците. В най-

добрия случай първата компетентна фирма ще подготви проучване, което другите ще копират и така ще могат да реализират печалба. Във всички случаи, този ненормално голям марж води до печалба за възложителя или за определените от него бенефициенти, като се използват черни каси и фалшиви фактури.

Фиктивни проучвания

Длъжностното лице може да поръча проучвания, за които да заплати на вноски (подобно заплащане може да достигне до 80 % от договорената сума още преди получаването на доклада от проучването; честа е практиката авансово да се изплаща половината от хонорара). Впоследствие ще се окаже, че е невъзможно да бъде получено поръчаното проучване поради различни причини: неспособността на консултанта да се справи със задачата, изчезването на консултантската фирма или поради факта, че поръчителят престава да се интересува от проучването (което междувременно е загубило значението си), даже и в случаите, когато фирмата, страна по договора, не е прекратила дейността си след като е инкасирала авансовата сума. Във всички тези случаи, авансовите плащания отиват при участниците в измамната схема (като резервният фонд се използва за изплащане печалбата на възложителя), тъй като наличните (фалшиви) фактури позволяват на фирмата контрагент да докаже, че плащанията съответстват на предоставените услуги, които са реализирали съответната печалба.

Проучвания, чиято стойност надвишава националния лимит

Ако стойността на дадено проучване надвишава официално определения лимит, възложителят може да организира тръжна процедура или „процедура по договаряне".

Заобикаляне на процедурата

В случай на провеждане на тръжна процедура, възложителят обикновено избира „най-изгодния икономически" проект, като удобен начин за селектиране на предварително набелязаната от него фирма. При това, той определя субективно допълнителни критерии за селекция, като например индивидуална компетентност на мениджърите, репутация на фирмата, предишни участия на фирмата в съответния регион и др. След като въведе тези допълнителни изисквания, възложителят с по-голяма сигурност успява да селектира „най-компетентната" фирма, отговаряща на неговите критерии.

Когато в случай на силна конкуренция заделените за проучването средства не са достатъчни, за да гарантират предварително определения марж, възложителят бива убеждаван от предварително избраната от него консултантска фирма да разшири параметрите на проучването, което ще доведе до по-добро изследване на резултатите от реализирането на предложения проект. Така възниква цяла спирала от промени в тръжния договор от страна на възложителя или определения от него консултант, при което се определят напълно произвол-

ни цени (като първоначално определените тарифи не се променят, но се увеличават часовете за положен труд). Подобни промени позволяват да се генерира допълнителен марж, който впоследствие ще бъде разпределен между възложителя и неговите приятели.

Променяне на резултата от селекцията

Възложителят може също така да избере най-ниската оферта в рамките на тръжната процедура. При подобно решение спечелилата фирма ще разполага с няколко възможности да плати комисиона на възложителя:

- Ако спечелилият участник в търга не е информиран за комисионата, която дължи на възложителя, той става жертва на изнудване от последния, който, въпреки че официално е селектирал неговата оферта, ще му разреши да започне реализацията едва след като получи съответната комисиона. Така спечелилият консултант е принуден да изплати последната, за да не бъде лишен от възможността да участва в бъдещи търгове. За да бъде в състояние да изплати неочакваната от него „комисиона", съответният консултант е принуден: а) да получи промяна в условията, чрез която да е в състояние да генерира нужната сума чрез фалшиви фактури; б) да намали собствения си марж, като отчете допълнителни фиктивни разходи (фалшиви фактури), за да избегне данъците върху фиктивната печалба; или в) да наеме незаконно работници или – в повечето случаи – да възложи на подизпълнител да извърши тази дейност.

Ако спечелилата фирма/консултант е била уведомена предварително за комисионата, тя ще е включила този разход в общата стойност на офертата си. При подобна хипотеза няма да има нелоялна конкуренция, тъй като всичките участници в търга ще бъдат третирани еднакво. Тук комисионата може да бъде платена на възложителя по класическия начин – използването на фалшиви фактури, което обикновено се извършва чрез приятелска консултантска фирма, която е специализирана в подобни транзакции. Възложителят налага подобна „приятелска" фирма да бъде записана като подизпълнител от страна на спечелилия търга още преди подписването на договора с последния. Въпросният подизпълнител получава щедро заплащане срещу надписани фактури в замяна на безполезни услуги, които не изискват специална техническа експертиза (в много случаи посредством манипулиране и „дообработка" на вече получените резултати от проучването). В крайна сметка, именно тези фактури ще бъдат използвани за обогатяването на възложителя.

В случаите, когато търговете надхвърлят общоевропейския лимит, съобщението за провеждане на тръжната процедура следва да бъде публикувано в „Официален вестник на Европейския съюз". В много от случаите, впоследствие възложителят използва тези процедури, за да възложи договора на най-удобния консултант. В други случаи, той определя субективно (чрез занижаване на резултатите), че търгът е бил провален, за да може да използва процедура по договаряне с

различни консултантски фирми и в крайна сметка да селектира „най-добрия" кандидат, т.е. онзи, който е известен със склонността си към използване на корупционни сделки. Подобна маневра е използвана и в рамките на национално проведен търг.

ЧАСТ 3. ИНСТРУМЕНТИ И ТЕХНИКИ ЗА РАЗСЛЕДВАНЕ И МЕТОДИКА НА РАБОТАТА

ИЗПОЛЗВАНЕ НА OSINT ПРИ РАЗСЛЕДВАНИЯ[21]

Разузнавателната информация от открити източници (OSINT) представлява публично достъпна информация, която се появява в печатен или електронен формат, включително: радио, телевизия, вестници, списания, интернет, търговски бази данни, както и видеоклипове, графики и чертежи.

Революцията при информационните технологии, търговията и политиката от края на Студената война прави отворените източници на информация все по-налични, повсеместни и ценни. Накратко, човек може да събере повече разузнавателна информация от открити източници, с по-голяма лекота и срещу по-ниски разходи, от когато и да било в миналото. Бумът на OSINT предизвиква трансформация в света на разузнаването, с появяването на открити версии на тайните методи за агентурно разузнаване (HUMINT), разузнаване чрез изображения (IMINT) и радиоелектронно разузнаване (SIGINT).

Един от най-важните инструменти за анализатора на OSINT са големите комерсиални търсачки, като например Google или Yahoo, както и различните онлайн платформи за социални медии като Facebook, Twitter и Youtube. Търсачките повишават ефективността на достъпа чрез техните алгоритми за индексиране и търсене, които могат за кратко време да обработват милиони страници данни и документи. Търсачките позволяват висока конкретика, например стесняване на търсенето до конкретни държави или домейни, публикувани книги или специализирана научна литература. Един опитен анализатор на OSINT знае къде е най-вероятно да открие най-качествена информация. Могат да се правят мащабни или тясно специализирани търсения с помощта на конкретни стратегии, благодарение на които да се извлече само най-подходящата информация. Това е етапът, където „аналитичният процес" започва.

В рамките на този процес, анализаторът идентифицира „констатации" (т.е. факти, които са му известни и които може да провери) и „пропуски" (неща, които знае, че не са му известни). OSINT често се използва в комбинация с други разузнавателни канали. Информацията от няколко източника и събрана с различни средства се синтезира от

---

[21] За основа служат документите: R. A. Norton. Ръководство за разузнаването от открити източници. Журнал за изследвания в разузнаването на САЩ, 18(2), 2011; Sean McKeown, David Maxwell, Leif Azzopardi и William Bradley Glisson. Разследване на хора: качествен анализ на поведението на анализаторите при търсене сред разузнавателна информация от открити източници. IIiX'14, Регенсбург, Германия: 26-29 август 2014.

обобщаващи анализатори, които съчетават различните видове информация и изграждат изчерпателен отговор на текущия казус, за кратко време и с голяма точност. Процесът има повтарящ се характер, тъй като с постъпването на нови констатации и несъответствия възникват нови въпроси.

Добрите анализатори на OSINT са специалисти по разрешаване на проблеми, които притежават специфични технически познания, като например специализирани езикови умения, експертен опит в областта на културата и/или науката, както и когнитивни умения. Анализаторите на OSINT, които осъществяват мониторинг на уебсайтове и блогове на съответния роден език и които свободно владеят езика и неговите диалекти, особено такива, свързани с проблемни региони от света, са особено ценени. Изискванията за специализирани умения за работа с OSINT се очаква да се увеличават в бъдеще, тъй като световната мрежа продължава да се разширява, а количеството на информацията продължава неимоверно да се увеличава.

Всеобхватният достъп до интернет доведе до трансформация на много аспекти на съвременното общество и до значителна промяна на начините, по които комуникираме и обменяме информация. Платформите на социалните мрежи, сайтовете за блогове и услугите за обмен на съобщения позволяват на отделни лица да разпространяват своите мисли в глобалната мрежа или да се изразяват по други начини онлайн. В резултат на всичко това, ние на практика публикуваме голямо количество биографична информация в интернет, с което потенциално я правим свободно достъпна за всеки, който иска да я потърси. Изследвания на търсенията в интернет показват, че някъде между 4 % и 10 % от търсенията съдържат име на лице, което показва, че до известна степен общественият интерес отразява търсенето на този вид информация. Действително, съществуват специализирани търсачки, създадени за намиране на хора в интернет пространството. Независимо дали търсенето се прави в специализирана или универсална търсачка, повечето запитвания се отнасят до непублични личности, а не за знаменитости.

Изглежда, че социалните мрежи играят голяма роля при търсенето на лица, като данните показват, че 66 % от запитванията, направени в специализираните търсачки за търсене на хора, водят до профили в социалните мрежи. Тези профили предлагат сведения за живота на хората, които може да не са налични чрез традиционните средства. В допълнение към това, потребителите на социални мрежи открито споделят чувствителна информация, като един ярък пример за това е широкоразпространеното популяризиране на престъпни групи от страна на техни млади членове. Въпреки това, едва 1 от 4 потребители на социалната медийна платформа Facebook е активирал ограничаващи настройки за поверителност, които намаляват обществената достъпност на тази информация – тези настройки сами по себе си не предотвратяват напълно събирането на информация относно потребителя.

В разузнавателната общност, сведенията, събрани от отворени източници на информация се наричат „разузнавателна информация от

открити източници" (OSINT). Добитата от тези източници информация, която включва обществено достъпна информация в социалните мрежи, може да се използва за най-различни цели. В някои случаи тя може да се използва незаконно, например за преследване, тероризъм или кражба на самоличността. Въпреки това, при наличие на подходящи правни и етични съображения, тези източници могат да се използват и за законни разследвания на OSINT, например: за проверка на служители, за разкриване на измами, за борба с тероризма и с организираната престъпност.

Каре 5. Пример за OSINT при действителни разследвания, AFIR, Румъния

Случай по подмярка 6.2 – ***Финансиране за къща за гости*** – има изискване финансираната дейност да бъде за нов обект, който преди това не е използван за земеделски/селски цели.

I. Приложение

Бенефициентът е кандидатствал за финансиране за промяна на предназначението на къща за живеене в къща за гости и нейната модернизация.

II. Разследващи мерки чрез OSINT, налични в интернет:

- Изображения от Google Street View показват, че преди подаване на заявлението за кандидатстване, къщата вече се е използвала като къща за гости.
- Открити са уебсайтове за туристически резервации, в които има отзиви от клиенти за техния престой в къщата за гости. От това става ясно, че имотът вече е ползван като къща за гости преди кандидатстването за финансова помощ.

III. Заключение – Проектът не отговаря на условията за подпомагане, а финансирането – отказано.

Видовете информация, която се търси, както и начините за нейното използване, могат да бъдат най-различни, в зависимост от контекста на разследването. В крайна сметка, информацията се събира, за да се изпълни конкретна задача. Пример за това е проверката на кандидат за високопоставена длъжност. В този случай е разумно да се извърши проверка за криминално минало, както и да се проучи общият характер, поведение и склонности на индивида, за да се избегнат бъдещи скандали.

По отношение на разследванията на терористични действия, личното поведение се разглежда в различен контекст, а при социалния елемент се обръща основно внимание върху свързаните лица. С кого говори този човек? Какво казва? По какъв начин комуникира? Къде ходи и какво върши? Този вид проучване може да доведе до разкритието, че субектът е свързан с известни терористи или открито публикува информация, свързана с екстремистки уебсайтове. В случай на потенциално корпоративно сливане, може да е разумно да се проучи историята на дружеството и неговите ръководни слу-

жители. В този сценарий могат да се използват общественодостъпни бизнес документи, които могат да разкрият дълга поредица от неуспешни стопански начинания, и така да покажат, че е неразумно да се извършва въпросното сливане. Във всички случаи, огромните масиви от открити източници на информация могат ефективно да се използват за определяне на курса на действие или за потвърждаване/опровергаване на дадено твърдение. Изобилието на информация в интернет, включително генерирано от потребителите съдържание, превръща анализирането на данни в сериозно предизвикателство. Следователно, за разследващите органи валидирането и проверката на информацията са от ключово значение за събирането на доказателствени данни.

СЪЗДАВАНЕ НА ПРОЦЕС ЗА ПРОВЕРКА И КОНТРОЛЕН СПИСЪК[22]

Основи на проверката

- Предварително изгответе план и въведете процедури за проверка.
- Проверката е процес. Пътят на проверката може да бъде много различен в зависимост от търсения резултат.
- Проверявайте източника и съдържанието, което предлага.
- Никога не повтаряйте машинално или не се доверявайте на източниците, независимо дали става дума за свидетели, жертви, извършители или органи на властта. Разказите на преките участници могат да бъдат неточни или манипулативни, подхранвани от емоции или изкривени от пропуски в запомнената информация или от ограничена перспектива.
- Проверявайте източниците, като задавате въпросите: „Откъде знаете това?" и „По какъв друг начин може да сте научили за това?"
- Правете тройно съпоставяне на тяхната информация с такава от други достоверни източници, включително документация, като например снимки и аудио/видео записи.
- Задавайте си въпроса: „Знам ли достатъчно, за да мога да потвърдя информацията?" Имате ли достатъчно познания по темите, които изискват разбиране на цялостния микс от културни, етични, религиозни аспекти?
- Работете в сътрудничество с членове на екипа и с експерти; не разчитайте само на себе си.

Проверка на генерирано от потребители съдържание

- Започнете от предположението, че съдържанието е неточно или е било оформяно, обработвано, третирано, дублирано и/или повторно публикувано в различен контекст.
- Следвайте тези стъпки при проверка на генерирано от потребителите съдържание:

[22] За основа служи документът: Наръчник за осъществяване на проверки. Европейски център за журналистика, 2014.

  - Идентифицирайте и проверете първоначалния източник и съдържанието (включително местоположение, дата и приблизителен час).
  - Правете тройно съпоставяне и проверка на източника.
  - Получете разрешение от автора/създателя за използване на съдържанието (снимки, видеоклипове, аудиозаписи).
- Винаги събирайте информация относно потребителите, които са качили съдържанието, и ги проверявайте възможно най-обстойно.

1. Идентифицирайте и проверете първоначалния източник и съдържанието (включително местоположение, дата и приблизителен час)

Произход

Първата стъпка при проверката на генерирано от потребителите съдържание е да се идентифицира оригиналното съдържание, като например съобщение в Twitter, изображение, видеоклип, текстово съобщение и др. Някои въпроси, с които е добре да се започне:

- Можете ли да откриете същия или подобни постове/съдържание на друго място в интернет?
- Кога е качена/заснета/споделена първоначалната версия?
- Можете ли да идентифицирате местоположението? Има ли генерираното от потребителя съдържание геолокация?
- Има ли уебсайтове, към които съдържанието предлага препратки?
- Можете ли да установите самоличността на лицето, което е споделило/качило генерираното от потребителя съдържание, и да се свържете с него/нея за допълнителна информация? (вж. по-долу раздела „Източник".)

Когато работите с изображения и видеоклипове, използвайте търсене на изображения в Google или TinEye, за да изпълните обратно търсене по мини-изображение (thumbnail) на дадено изображение/видеоклип. Ако излязат няколко препратки за едно и също изображение, натиснете върху „view other sizes" (преглед на други размери), за да откриете най-високата налична резолюция/размер, която обикновено е на оригиналното изображение.

За проверка на произхода на изображения:

- Използвайте търсене на изображения в Google или TinEye, за да изпълните обратно търсене по мини-изображение (thumbnail) на дадено изображение. Ако излязат няколко препратки за едно и също изображение, натиснете върху "view other sizes" (преглед на други размери), за да откриете най-високата налична резолюция/размер, която обикновено е на оригиналното изображение.
- Проверете дали изображението съдържа EXIF данни (метаданни). Използвайте софтуер като Photoshop или безплатни инструменти като Fotoforensics.com или Findexif.com, за да видите информация за модела на фотоапарата, времевия отпечатък на изображението

(обърнете внимание: датата може по подразбиране да показва зададените от производителя настройки) и размерите на оригиналното изображение.
- Социалните мрежи, като Twitter, Facebook и Instagram премахват повечето метаданни. Flickr е изключение. Вместо тях, опитайте чрез Geofeedia и Ban.jo да идентифицирате GPS данните от мобилното устройство, което е използвано за качване на изображението.

За проверка на произхода на видеоклипове:

- Използвайте съкращения, имена на места и други местоимения за добро търсене по ключови думи в платформите за споделяне на видеоклипове като YouTube, Vimeo и Youku.
- Използвайте Google Translate, когато Ви се налага да работите със съдържание на чужд език.
- Използвайте филтър по дата, за да откриете най-ранните видеоклипове, които отговарят на ключовите думи.
- Използвайте търсене на изображения в Google или TinEye, за да изпълните обратно търсене по мини-изображение (thumbnail) на видеоклип.

Източник

След като сте идентифицирали оригиналното съдържание, съберете информация относно автора/създателя на съдържанието. Целта е да потвърдите дали лицето, стоящо зад профила, е надежден източник.

Разгледайте цифровия отпечатък на лицето, качило съдържанието, като зададете следните въпроси:

- Можете ли да потвърдите самоличността на лицето и да се свържете с него?
- Запознати ли сте с този профил? Били ли са съдържанието и съобщената информация надеждни в миналото?
- Проверете историята на лицето, качило съдържанието, в социалната мрежа:
  - Колко е активно в този профил?
  - За какво говори, какво споделя?
  - Каква биографична информация е видна в профила? Прави ли препратки към други места?
  - Какъв вид съдържание е качвал този потребител преди това?
  - Къде е базиран потребителят, ако се съди по историята на профила?
- Проверете с кой е свързан в социалната мрежа:
  - Кои са неговите приятели и последователи?
  - Кого следва той?
  - С кого си общува?
  - Присъства ли в списъците на някой друг?
- Опитайте се да откриете други профили, свързани със същото име/потребителско име в други социални мрежи, за да откриете допълнителна информация:

  - Ако откриете истинско име, използвайте инструменти за търсене на хора (Spokeo, White Pages, Pipl.com, WebMii), за да откриете адреса, електронната поща и телефонния номер на човека.
  - Проверете други социални мрежи, например LinkedIn, за да разберете повече за професионалната история на човека.
- Проверете дали даден потвърден профил в Twitter или Facebook действително е верифициран, като поставите показалеца на мишката над синята отметка. Ако профилът е верифициран от Twitter или Facebook, информацията, която ще се появи, ще гласи: "Verified Account" (верифициран профил) или "Verified Page" (верифицирана страница).

Когато работите с изображения и видеоклипове, вземете предвид гледната точка на човека, който е заснел кадъра/клипа. (Тези въпроси работят и за проверка на текстова информация) Задайте си следните въпроси относно източника, за да проверите неговата правдоподобност:

- Кой е това?
- Къде се намира?
- Как се е озовал там?
- Какво е бил в състояние да види (и какво показва неговата снимка/видеоклип)?
- Къде е застанал?
- Защо е точно там?

Свържете неговата дейност с тази на всички други онлайн профили, които той поддържа, като зададете следните въпроси:

- Пуснете търсене в Twitter или Facebook на уникалния код на видеоклип – дали това не са свързани профили?
- Съществуват ли други профили – Instagram, блог или уебсайт – които да са посочени във видео профила или по друг начин да са свързани с лицето, качващо видеоклипа?
- Каква информация дават свързаните профили за скорошно местоположение, дейност, надеждност, склонности или дневен ред?
- Колко дълго са били активни тези профили? Колко активни са били? (Колкото по-дълго или повече са били активни, толкова по-вероятно е да са надеждни.)
- Кои са профилите в социалните медии, които са свързани с лицето, качило съдържанието, и какво ни казват те за него?
- Можете ли да откриете WHOIS-информация за свързан сайт?
- Има ли посочено лице в местните телефонни указатели, в Spokeo, Pipl.com, WebMii или LinkedIn?
- Показват ли техните онлайн социални кръгове, че са близо до тази история/това местоположение?

Съдържание

Дата

Проверете датата и приблизителното време, особено при работа със снимки/видеоклипове:

- Проверете информацията за деня и местоположението, където се е случило събитието. Метеорологичните условия същите ли са като тези в (местните) прогнози за времето и тези при друго качено съдържание от същото събитие? Използвайте Wolfram Alpha за търсене (например „Какво е времето в Лондон, Англия, на 20 януари 2014 г.?").
- Претърсете новинарските източници за репортажи относно събитията на този ден.
- Като използвате търсене на видеоклипове и изображения (YouTube, Google, TinEye и др.), вижте дали някоя по-ранна част от съдържанието от същото събитие не предшества Вашия пример. (Имайте предвид, че за времевите отпечатъци YouTube използва часа по часовата зона „Тихоокеанско стандартно време" от момента, в който започва качването на видеоклипа.).
- За изображения и видеоклипове, търсете (и слушайте за) идентифициращи елементи, които показват датата/часа, като например часовници, телевизионни екрани, страници от вестници и др.

Местоположение

Друг много важен аспект от проверката е да идентифицирате местоположението на съдържанието:

- Съдържанието съдържа ли автоматична информация за геолокацията? (Услуги като Flickr, Picasa и Twitter предлагат опция за включване на местоположението, макар че тя не винаги е 100 % надеждна.).
- Открийте отправни точки за сравнение със сателитни снимки и снимки с ясна геолокация, като например:
  - Табели/надписи върху сгради, пътни знаци, регистрационни номера на автомобили, билбордове и др. Използвайте Google Translate или free.orc.com за онлайн превод.
  - Отличителен уличен пейзаж/ландшафт, като например планински вериги, линия на дърветата, отвесни скали, реки и др.
  - Забележителности и сгради като например църкви, минарета, стадиони, мостове и др.
- Използвайте Google Street View или Google Maps и по-специално тяхната функция „Снимки", за да проверите дали снимките с геолокация отговарят на местоположението на изображението/видеоклипа.
- Използвайте Google Earth за проучване на стари изображения/видеоклипове, тъй като там има история на сателитните изображения. Използвайте изгледа „терен" в Google Earth.
- Използвайте Wikimapia, която представлява клаудсорсинг версия на Google Maps, за идентифициране на забележителности.

- Използвайте метеорологичните условия, като например слънчева светлина или сенки, за да установите приблизителния час от денонощието. Използвайте Wolfram Alpha за търсене сред прогнозите за времето за конкретно място и конкретен ден и час.
  - Регистрационен номер на превозното средство/номер на шофьорска книжка.
  - Облекло.

За видеоклипове:

- Обърнете внимание на езика (езиците), които се говорят във видеоклипа. Проверете дали акцентите и диалектите отговарят на географското местоположение. Имайте предвид, че Google Translate не предлага точен превод за някои езици. Поискайте помощ от някой, който говори съответния език.
- Има ли последователност при описанията на видеоклиповете и дали са предимно от конкретно местоположение?
- Имат ли видеоклиповете дата?
- Ако видеоклиповете в профила използват лого, дали има последователност на това лого при различните видеоклипове? Отговаря ли то на аватара в профила в YouTube или Vimeo?
- Дали лицето, качващо съдържанието, „изрязва" видеоклипове от новинарски организации и от други профили в YouTube или качва единствено генерирано от потребителя съдържание?
- Дали лицето, качващо съдържанието, пише на жаргон или диалект, който може да се идентифицира в разказа във видеоклипа?
- Дали видеоклиповете в този профил са с постоянно качество? (В YouTube отидете в „Настройки" и после в „Качество", за да определите най-доброто налично качество.).
- Описанията на видеоклиповете имат ли файлови разширения, като например .AVI или .MP4 в заглавието на видеоклипа? Това може да показва, че видеоклипът е качен директно от дадено устройство.
- Описанието на видеоклипа в YouTube включва ли подобен текст: "Uploaded via YouTube Capture" (качено чрез YouTube Capture)? Това може да показва, че видеото е заснето със смартфон.

2. Триангулация и проверка на източника

След като преминете през горните стъпки, се запитайте:

- Дали идеята на изображенията/видеоклиповете/съдържанието отговаря на контекста, в който са заснети?
- Има ли нещо, което изглежда не на място?
- Има ли случаи на конфликт между подробната информация за източника и отговорите на моите въпроси?
- Има ли нещо в Snopes[23], свързано с това?
- Изглежда ли нещо не наред, или пък е твърде хубаво, за да е вярно?

[23] Интернет страница за проверка на факти и твърдения.

Когато се свързвате с източника, задайте директни въпроси и въпроси за кръстосана справка с информация, която вече Ви е станала известна в хода на проучването. Уверете се, че техните отговори съвпадат със собствените Ви констатации.

За изображения:

- Когато задавате въпроси, отразявайте това, което знаете от EXIF-данните и/или информацията за геолокация от инструменти като Google Street View и Google Maps.

За видеоклипове:

- Ако имате съмнения относно структурата на видеоклипа, използвайте софтуер за редактиране, като например VLC Media Player (безплатен), Avidemux (безплатен) или Vegas Pro (с лиценз), за да разделите даден видеоклип на съставните му фреймове.

СКАНИРАНЕ НА ХОРИЗОНТА[24]

Управлението на измамите е деликатна област във всяка една сфера. Въпреки че технологичните пейзажи добавят усложняващи елементи при предотвратяването на измами, плътно интегрираните системи, подкрепяни от непрозрачни и неефикасни процеси, също не са добър вариант. **Ранното откриване на измамите и ясното разбиране на схемите за измама** играят ключова роля за предотвратяването им.

В исторически план вниманието е било съсредоточено върху системи за непрекъснат мониторинг в реално време и с тяхното прилагане са засичани злонамерените дейности. Анализите са използвани в най-добрия случай за установяване на „тенденции" от натрупаните обемни исторически масиви с данни. Въпреки това, предвид увеличаващата се „креативност" сред извършителите на измами, се смята, че анализите и машинното обучение, подпомагани от програма за сканиране на хоризонта, могат да постигнат отлични резултати по отношение на идентифицирането на схеми за измама и техните проявления.

Например, има измами, които обикновено обхващат процеси и отдели в организации, може би дори географски области. В подобни случаи борбата чрез традиционните методи се превръща в дълъг процес, при който комисия от експерти прави оценка на сценария на измамата и инициира евентуални коригиращи действия. Ако се

[24] За основа служат следните документи: Ключовата триада за предотвратяване на измами: сканиране на хоризонта, анализи и машинно обучение, Бяла книга. Tata Consultancy Services; Модели за сканиране на хоризонта: как да се интегрира сканирането на хоризонта в европейските политики за научни изследвания и иновации. Европейска комисия, 2015; Сканиране на хоризонта в управлението: концепция, опит на държавите и модели за Швейцария. Цюрих: Център за изследвания в сферата на сигурността, 2009.

окаже, че това е първи случай на този вид измама за съответната институция, процесът може да продължи дори още по-дълго, което означава, че се губи ценно време, което може да се използва за ограничаване на щетите и предотвратяване на следващ подобен случай.

В допълнение към това, екипите за предотвратяване на измами разполагат с по-малко ресурси, а от тях се изисква да имат множество различни умения. За проактивно идентифициране на измами в реално време, количествен анализ и предотвратяване, организациите трябва да прилагат инструменти за автоматизация, базирани на интелигентни технологии, като например машинното обучение и анализите, в координация с техники за сканиране на хоризонта.

Сканирането на хоризонта представлява систематичен подход за откриване на ранни признаци на потенциално важни събития. Те могат да бъдат слаби (или ранни) сигнали, тенденции, прикрити бъдещи заплахи или други събития, устойчиви проблеми, рискове и заплахи, включително въпроси, които се намират на границата на сегашния начин на мислене, които могат да бъдат предизвикателство за изразени в миналото предположения. Сканирането на хоризонта може да бъде напълно проучвателно и отворено или да бъде ограничено търсене на информация в конкретна област, съобразно целите на съответните проекти или задачи. То се стреми да определи какво е постоянно, какво може да се промени и какво постоянно се променя във времевия хоризонт, който е обект на анализа. Различни критерии се използват при процеса на търсене и/или филтриране. Времевият хоризонт може да бъде краткосрочен, средносрочен или дългосрочен. Данните за сканирането на хоризонта включват както „меки данни" (мнения, колективни прозрения или разузнавателна информация) така и „твърди данни" (структурирани данни от транзакции, обикновено от „системни записи").

С все по-повсеместната цифровизация на процесите, на организациите се налага да свързват техните „системи за действие" с техните „системи за записване", за да могат да откриват измами на равнище свързващи елементи. Един от ключовите аспекти на сканирането на хоризонта е възможността да се забелязва неочакваното посредством проучвателно прогнозиране. Изследването на познати модели чрез анализ на сценарии и нормативно прогнозиране следва да се допълва с техники за сканиране на хоризонта, което често включва откриване на тенденции и идентифициране на елементите, които са постоянни, тези, при които се наблюдава промяна и тези, които постоянно се променят.

Разкриването на измами е преминало към непрекъснат мониторинг в реално време на операциите и използването на инфраструктурата с цел идентифициране на необичайно поведение. Преди това са се използвали традиционните методи за извършване на одитни проверки и свързването им с несъответствия във финансовите отчети. Техниките и инструментите за предотвратяване на измами се нуждаят от възможности за предвиждане и предотвратяване на „неизвестното",

което може да се постигне чрез събиране на данни за хоризонта, части от които могат първоначално да изглеждат несвързани.

Статистически техники могат да дадат ценна информация за възможните и вероятните сценарии за измами. Отделно от това, подаването на данните към възможните вътрешни сценарии и определянето на вероятността от тяхното проявление, вземайки предвид съответните фактори на бизнес средата и вътрешния контрол за съответната организация, е важна практика. Следователно, данните от сканирането на хоризонта помагат за постигане на вътрешно разбиране за възможните сценарии за измами, които преди това не са присъствали върху радара на организацията, тъй като не е провеждана съпоставка и не са били разпознати като възможни. Редовното съпоставяне на данни за хоризонта с вътрешни данни ще помогне на организацията да премине от режим на откриване на измами към режим на предотвратяване на измами.

Развитието на алгоритми за машинно обучение, приложими за сценариите, или комбинации от тях, както и валидирането им с подходящи набори от данни, ще позволи автоматизиране на предотвратяването на измами и системите за ранно предупреждение. Силата на такъв подход произлиза от обстоятелството, че той едновременно ще обхване областите: бизнес, операции и технологии. Уместността на алгоритмите трябва да се валидира в този контекст от експерти по съответните теми, за да могат организациите да избират правилните предупреждаващи сигнали и техните взаимовръзки. Ненастъпването на тези сценарии е желаният резултат при предотвратяването на измами.

Оттам нататък, когато бъдат получени нови данни от сканиране на хоризонта, сценариите и техните случайни комбинации се анализират отново, за да се предскажат възможностите за измами. Когато бъдат получени сигнали от системата за ранно предупреждение, трябва да бъдат активирани съответните промени в съществуващите фактори на бизнес средата и вътрешния контрол, за да се предотврати възникването на измами. Системата се „учи" при всеки нов набор от данни и „разузнавателните" ѝ възможности прогресивно нарастват.

Сканирането на хоризонта е ефикасен начин за събиране на данни от голям брой предприятия, които използват подобни архитектури, услуги или бизнес модели. Тази техника помага за преодоляване на недостатъците на наличните данни при разработване и валидиране на сценарии, като се използват уроците от цялата екосистема за създаване на експоненциална стойност за организацията. Нови набори от данни, които досега са изглеждали неуместни за организацията, могат да се окажат ценни в някой нов сценарий или контекст на развитие. Облачните технологии помагат за съпоставянето и анализирането на големи набори от данни за бизнес употреба при достъпни разходи за използване и поддръжка – в комбинация с анализи и машинно обучение, това може да улесни развитието на интелигентен и основан на данните подход към предотвратяването на измами. Такъв подход ще позволи на организациите проактивно да възпри-

емат технологични иновации без страх от измами, произтичащи от техните системи, процеси и служители. Като се имат предвид тези предимства, организациите трябва активно да обмислят използване на ключовата триада: сканиране на хоризонта, анализи и машинно обучение, за развитието на футуристичен подход към предотвратяването на измами в една ера, която се характеризира с иновативни технологии и бизнес модели.

В по-тесен смисъл, сканирането на хоризонта се отнася до инструмент на политиката, който систематично събира информация относно нововъзникващи проблеми и тенденции в политическата, икономическа, социална, технологична и екологична среда на дадена организация. В по-глобален смисъл, то се използва и като синоним за различни така наречени „дейности за предвиждане", чиято цел е развитие на възможностите на организациите за по-ефективно справяне с неясното и сложно бъдеще.

На преден план изпъкват две ключови функции за формирането на политики:

- *Информационна функция*: Сканирането на хоризонта информира хората, отговарящи за формиране на политиките, относно нововъзникващите тенденции и развития във външната среда на дадена организация. Неговите основни резултати са стратегически сканирания, които обхващат широка гама от въпроси и се разпространяват под формата на резюмета на политики, доклади и сценарии.
- *Функция за развитие на политики*: Сканирането на хоризонта се отнася до процес, който подкрепя създаване на визия за желаното бъдещо развитие и подчертава значението на създаването на мрежи и потоци от познания между хората и организациите. Интензивните взаимодействия сред професионалните общности и тези, занимаващи се с формирането на политиките, стимулират появата на споделени разбирания и така улесняват развитието на иновативни политики.

ПРИЛОЖЕНИЕ В ПРАКТИКАТА

Сканирането на хоризонта с цел откриване и събиране на доказателства относно външната среда на дадена организация представлява само една (макар и важна) част от цялостния процес на предвиждане на бъдещите събития, който е описан по-подробно в следващите параграфи. Предвиждането на бъдещото развитие се дефинира като преднамерен опит за разширяване на „границите на възприятията ни". То разширява осведомеността ни за нововъзникващи въпроси и ситуации, и подкрепя стратегическото мислене чрез създаване на палитра от различни начини, по които бъдещето може да се развие. Процесът на предвиждане може най-общо да се раздели на три фази:

- *Ранно откриване* на нововъзникващи въпроси с помощта на сканиране на хоризонта
- *Генериране на прогнози за бъдещето* чрез предприемане на бъдещи проекти
- Разработване на опции за политики чрез прилагане на *сценарийни техники*

Ранното откриване (Фаза 1) се занимава с идентификацията и непрекъснатия мониторинг над всички актуални въпроси и развития във външната среда на дадена организация. Концептуалната идея е да се създаде система за събиране на информация, която открива случаите на непоследователност в тенденции, които до преди това са считани за стабилни и непроменливи. Тези случаи на непоследователност обикновено се предшестват от „слаби сигнали", които подсказват за промените дълго преди за тях да разберат повечето хора и преди да им бъде обърнато внимание от хората, които определят политиките. От методическа гледна точка, това е надграждане над сканирането на хоризонта и разчита на предположението, че продължителното натрупване на информация позволява на наблюдателя да извлече по-ясни доказателства. Ранното откриване се очаква да подобри гъвкавостта на управлението, тъй като то намалява „изненадващите ефекти" и увеличава пространството за маневриране като дава на хората, които вземат решения, достатъчна преднина, за да предприемат подходящи мерки за противодействие срещу нововъзникващите заплахи.

Генерирането на прогнози за бъдещето (Фаза 2) се занимава с оценката и разбирането на избрани предизвикателства, свързани с политиките. След като информацията бъде сканирана, събрана, филтрирана и обработена, събраните доказателства се подлагат на тълкуване, за да бъдат разкрити „последиците от различните възможни бъдещи възгледи за определена организация". Конкретни въпроси, които могат да станат по-важни в бъдеще, се избират и се изучават в дълбочина. Изборът на въпроси се основава на конкретни критерии: те следва, например, да имат високо потенциално въздействие върху обществото и икономиката, да се активират от нови технологии, или да представят области, в които промените са сложни и бързи, а бъдещите развития са много несигурни. Друг често срещан важен набор от критерии е политическата подкрепа, предлагана от правителството и другите участници, които отговарят за вземането на решения, за да се гарантира, че новите прозрения по-късно ще доведат до политически действия. Подобни „бъдещи проекти" трябва да са базирани на най-добрите налични научни и други доказателства и да се опитват да уловят конкретен въпрос във всички негови приложими измерения. Няколко бъдещи проекта могат да текат едновременно и да разрешават широка гама от проблеми на политиката. Тяхната крайна цел е да обрисуват реалистична картина на „сегашните отражения на възможни бъдещи събития".

Прозренията, генерирани чрез бъдещи проекти водят до развитието на възможности за политиките (Фаза 3). Тъй като не съществува една версия на „бъдеще", се разглеждат различни потенциални

варианти за бъдещето, тъй като при условията на „повишена несигурност", най-добрият начин за действие е целенасочено да се гледа напред и да се представят „алтернативни сценарии". Сценариите могат да се разграничават като възможни, допустими, вероятни и предпочитани форми на бъдещо развитие, всички от които влизат в рамките на „конуса на възможното бъдеще":

- Възможните варианти за бъдещето включват всичко, което можем да си представим, независимо колко невероятно ни се струва, вкл. резултатите от знанията, които все още нямаме, но с които можем да се сдобием в някакъв бъдещ момент.
- За правдоподобните варианти за бъдещето има разумна вероятност да се случат, тъй като те отговарят на текущите общи познания и разбиране за това как работи светът.
- За вероятните варианти за бъдещето има достатъчна вероятност да се случат, тъй като те до голяма степен представляват екстраполации на настоящето и миналото в бъдещето.
- Накрая, за разлика от описаните по-горе варианти за бъдещето, предпочитаното бъдеще не е резултат от съществуващи (или не) познания, а е базирано на субективни оценки и ценности, които описват желаните резултати, предпочитани от отделни лица или организации.

Предпочитаните варианти за бъдещето се оформят чрез разработване на нормативни сценарии, в които се изследват аспекти на желаните политики. Въпреки това, формулирането на широко споделен консенсус относно предпочитаните варианти за бъдещето рядко е възможно в рамките на обществената политика, тъй като обсъждане сред много заинтересовани страни с много разнообразни интереси и ценности почти неизбежно води до противоречащи си препоръки. Следователно, изграждането на нормативни сценарии следва да се разбира като отворен дискурс, който позволява взаимодействие и комуникация сред участниците и в крайна сметка води до взаимно разбиране за идеите на останалите страни за предпочитаното от тях бъдеще.

Кои са по-общите практически ползи от сканирането на хоризонта и предвиждането на бъдещето от гледна точка на определяне на политиката? Описаният по-горе процес косвено води до две функции, които са свързани с две различни значения на „сканиране на хоризонта".

Първата функция е информиране на политиката чрез осигуряване на познания и нови идеи, водещи до осезаеми резултати, като например доклади, резюмета на политики или сценарии относно новопоявяващи се въпроси.

В основата ѝ стои сканирането на хоризонта: аналитична задача за систематично събиране и документиране на данни и факти относно потенциално значими тенденции и развития в осезаемата политическа, икономическа, социална или технологична среда на дадена организация. Въпреки че подобен ориентиран към резултатите подход отдавна се счита като основна цел на сканирането на хоризонта, той

все повече се критикува като твърде статичен и не достатъчно полезен за процеса на социално обучение, който позволява създаването на ориентирани към бъдещето политики.

Следователно, фокусът вече се е изместил върху втората функция на предвиждането на бъдещото развитие, която улеснява разработването на иновативни политики. Предвиждането на бъдещото развитие се възприема като процес на учене, който подкрепя очертаването на желаните характеристики. Твърди се, че истинската сила на предвиждането на бъдещото развитие се крие в създаването на връзки, мрежи или потоци от знания между хората и организациите. С други думи: изготвянето на политики може да се подобри не само чрез конкретни продукти, но също и чрез подобряване на комуникацията, разширяване на мрежите, координация на предпочитанията и промени в мисленето. Тези подобрения позволяват на хората, които определят политиките, да правят информирани избори, да усъвършенстват политическата реакция и да улесняват създаването на политики. Тази ориентирана към процесите перспектива относно сканирането на хоризонта е уловена от изчерпателния процес на предвиждане на бъдещото развитие.

Следователно, потенциалните ползи от сканирането на хоризонта и предвиждането на бъдещото развитие са в две направления: традиционният, ориентиран към резултатите фокус върху „предоставянето на информация относно бъдещото развитие като основа за определяне на приоритетите", от една страна, и фокусът върху иновативен рефлексивен процес на взаимно обучение сред хората, определящи политиките, който стимулира „появата на общи визии", от друга страна.

ПРИЛОЖЕНИЕ 1. КОМПЮТЪРНИ ЕЛЕКТРОННИ ДОКАЗАТЕЛСТВА[25]

Информационните технологии непрекъснато се развиват и всяко ново развитие намира по-голяма роля в нашия живот. Възстановяването на доказателства от електронни устройства вече е неразделна част от разследващата дейност, както в публичния, така и в частния сектор. Електроните доказателства са ценни доказателства и следва да се третират по същия начин като традиционните съдебни доказателства – с уважение и грижа. Методите за възстановяване на електронни доказателства запазват доказателствената приемственост и цялост, но в същото време могат да изглеждат сложни или скъпи. Въпреки това, опитът показва, че ако с тях се работи правилно, резултатът е доказателства, които са едновременно убедителни и рентабилни.

Важно е да се отбележи, че правилата за доказателствата са приложими в еднаква степен за компютърните електронни доказателства и за материалните доказателства, получени от други източници. Винаги на отговарящото за конкретния случай длъжностно лице се пада отговорността за гарантиране на спазването на законите, по-специално за гарантиране, че използваните процедури за изземване на имущество се изпълняват в съответствие с действащото законодателство.

Представените тук насоки са формулирани в помощ на разследващите служители, които включват високотехнологичен елемент, както и за гарантиране на събирането на всички приложими доказателства – своевременно и по подходящ начин.

ПРИНЦИПИ НА КОМПЮТЪРНИТЕ ЕЛЕКТРОННИ ДОКАЗАТЕЛСТВА

Принцип 1:

Никое действие на правоприлагащите органи или техните служители не трябва да води до промяна на данните, съхранявани на даден компютър или носител на информация, на които в последствие може да се разчита в съда.

---

[25] За основа служи документът: *Ръководство за добри практики при компютърните електронни доказателства*. Обединено кралство: Работна група по електронните престъпления, Асоциация на началниците на полицейски участъци, 2014.

Принцип 2:

При обстоятелства, при които дадено лице смята за необходимо да получи достъп до оригинални данни, съхранявани върху компютър или върху носител на информация, то трябва да бъде компетентно за тази операция и да може да представи доказателства, с които да обясни приложимостта и последиците от своите действия.

Принцип 3:

Следва да бъде създадена одитна пътека или друг запис за всички процеси, които са приложени спрямо компютърните електронни доказателства. Независима трета страна следва да може да прегледа тези процеси и да постигне същия резултат.

Принцип 4:

Лицето, което отговаря за разследването (длъжностно лице по делото) носи цялостна отговорност за гарантиране спазването на закона и на тези принципи.

Обяснение на принципите

При електронните доказателства важат същите правила и закони, които са в сила и за документалните доказателства. Обосновката на документалната доказателствена стойност може да се опише по следния начин: тежестта на доказване се носи от обвинението, което трябва да може да покаже в съда, че представените доказателства не са били променяни или изменяни от момента, в който са преминали във владение на разследващите.

Операционните системи и другите програми често променят или добавят към съдържанието на електронните носители на информация. Това може да се случи автоматично, без непременно потребителят да разбере, че данните са променяни. За да се спазят принципите на компютърните електронни доказателства, когато е приложимо следва да се запазва изображение на цялото целево устройство. Частичното или селективно копиране на файлове може да се разгледа като алтернатива при определени обстоятелства, например когато обемът на данните, на които трябва да се запази точно изображение, го прави непрактично. Въпреки това, разследващите следва да внимават да запазят всички приложими доказателства, ако прилагат този подход.

В по-редки случаи, може да не е възможно да се получи точно изображение с помощта на разпознато устройство за създаване на изображения. При тези обстоятелства, може да бъде необходим достъп до оригиналната машина за възстановяване на доказателствата. Като се има предвид това, е от съществено значение

всякакъв подобен достъп да се осъществява от свидетел, който е компетентен да дава показания пред съда.

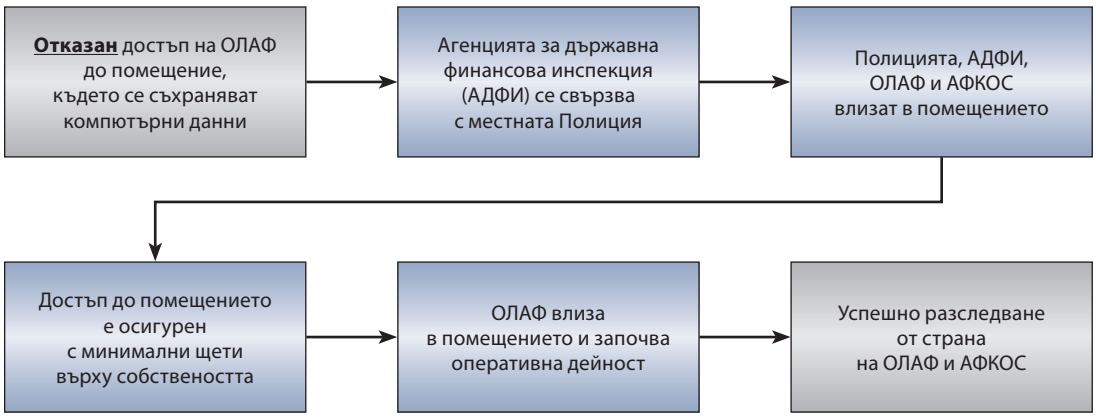
Изключително важно е да се покаже обективност в съда, както и последователност и цялост на доказателствата. Също така е необходимо да се покаже как доказателствата са били записани, като се демонстрира процесът, чрез който доказателствата са придобити. Доказателствата следва да бъдат запазени до такава степен, че трето лице да може да повтори същия процес и да получи същия резултат като този, представен пред съда.

ПРЕГЛЕД НА КОМПЮТЪРНИТЕ ЕЛЕКТРОННИ РАЗСЛЕДВАНИЯ

Технологиите присъстват във всеки аспект на съвременния живот. Имало е време, когато един компютър е запълвал цяла стая. Днес компютърът може да се побере в човешка длан. Престъпниците се възползват от същия този технологичен напредък, който служи като двигател на еволюцията на обществото.

Компютрите могат да се използват за извършване на престъпление, могат също да съдържат доказателства за престъпление или да бъдат обект на престъпление. Изключително важно е да разбираме ролята и характера на електронните доказателства, които могат да се намерят, как е правилно да се обработва местопрестъпление, което съдържа потенциални електронни доказателства и как дадена институция може да реагира на такива ситуации.

Фигура 6. Предизвикателства при получаването на цифрови доказателства в България: отказан достъп до помещения



Източник: *На база презентации по време на Конференцията.*

Настоящото ръководство представя колективния опит на правоприлагащите органи, академичните среди и частния сектор по отношение на признаването, събирането и съхранението на компютърни електронни доказателства при различни сценарии на престъпления.

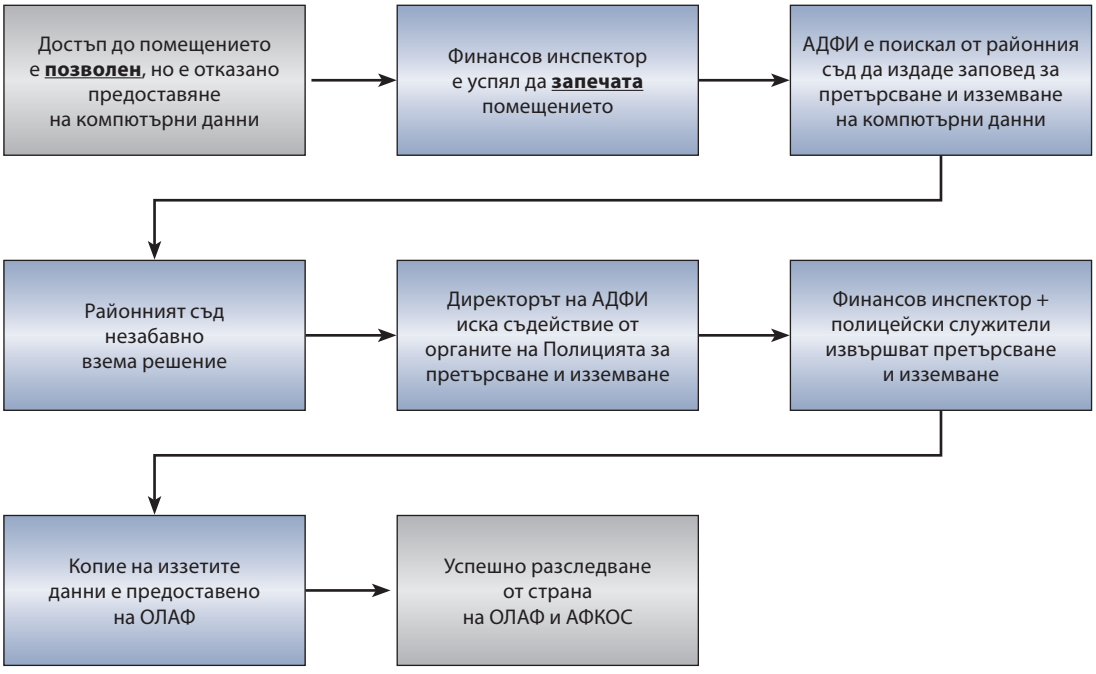
Всеки участник трябва да разбира деликатното естество на компютърните електронни доказателства и принципите и процедурите, свързани с тяхното събиране и опазване.

Характер на компютърните електронни доказателства

Компютърните електронни доказателства са относимите при разследвания информация и данни, които могат да се съхраняват и предават посредством компютър. Те представляват скрити доказателства, по същия начин, както пръстовите отпечатъци или ДНК данните (дезоксирибонуклеинова киселина).

В естественото му състояние, не можем да видим какво се съдържа във физическия обект, който съдържа нашите доказателства. Необходими са оборудване и софтуер за предоставяне на доказателствата. Може да бъдат необходими свидетелски показания, за да се обясни проверката и евентуалните ограничения на процеса. Компютърните

Фигура 7. Предизвикателства при получаването на цифрови доказателства в България: отказ на електронни данни



Източник: *На база презентации по време на Конференцията.*

електронни доказателства са деликатни по естество. Те могат да бъдат променени, повредени или унищожени при неправилно боравене или неправилно изследване. По тази причина, трябва да се вземат специални предпазни мерки за документиране, събиране, запазване и разглеждане на този вид доказателства. При неспазване на това изискване, е възможно доказателствата да станат неизползваеми или да доведат до неточно заключение.

В това ръководство се предлагат методи, които ще помогнат за запазване на целостта на такива доказателства.

Местопрестъпления

Съществуват много устройства/носители на информация, съдържащи данни, които могат да се срещнат при осъществяване на търсене по време на разследвания. Те често са ценни източници на доказателства, които, ако с тях се работи по подходящ начин, могат да разширят разследването. Този раздел е предназначен да помогне на лица, които не са получили специализирано обучение в тази област, за осъществяване на такова търсене и гарантиране на правилни действия във връзка с изземването на такъв материал.

Следващите насоки се отнасят до повечето от възможните сценарии в практиката. Общите принципи, ако бъдат спазени, ще гарантират най-добри шансове за събиране на доказателства в незамърсен и следователно приемлив вид.

Приема се, че в зависимост от конкретните обстоятелства по време на претърсване, може да има и по-уместни варианти от тези, които са представени по-долу. Въпреки това, тези алтернативни варианти няма да бъдат представени в това ръководство, тъй като такива начини на действие следва да се използват само от лица, които са получили съответното обучение в тази специализирана сфера на работа.

Повечето компютри, които се откриват при претърсване, са настолни персонални компютри или лаптопи.

Ако имате някакво съмнение за това какви са правилните действия, които следва са предприемете, потърсете съвет от специалист.

Настолни компютри и лаптопи

При откриване на компютърно оборудване, което изглежда изключено:

- Обезопасете и поемете контрол върху зоната, в която се намира оборудването.
- Преместете хората далече от компютрите и от източниците на захранване.
- Направете снимки или видеоклип на помещението и на всички компоненти в рамките на обекта, включително захранващите ка-

бели. Ако не разполагате с фотоапарат, начертайте план-скица на системата и поставете етикети на портовете и кабелите, за да можете да възстановите системата на по-късен етап.
- Дайте възможност на принтерите да завършат разпечатването.
- При никакви обстоятелства не включвайте компютъра.
- Уверете се, че компютърът е изключен – някои скрийнсейвъри могат да създадат впечатление, че компютърът е изключен, но светлинните индикатори за работата на харддиска и монитора може да показват, че машината все още е включена.
- Имайте предвид, че някои лаптопи може да се стартират при отваряне на капака.
- Отстранете основната захранваща батерия от лаптопите. Въпреки това, преди да го направите, преценете дали машината не е в режим на готовност. При такава ситуация, махането на батерията може да доведе до предотвратима загуба на данни.
- Изключете захранването и останалите устройства от гнездата на самия компютър (т.е. не от контакта). Един компютър, който привидно е изключен може да се окаже в спящ режим и така да позволява отдалечен достъп, съответно промяна или изтриване на файлове.
- Поставете етикети върху портовете и кабелите, за да можете да възстановите компютъра на по-късен етап.
- Уверете се, че всички елементи са подписани и са попълнени етикетите, прикачени към тях. Ако не направите това, можете да създадете трудности с приемствеността и в резултат на това оборудването да бъде отхвърлено за целите на съдебните експерти.
- Претърсете мястото за дневници, тетрадки или листове хартия с пароли – такива често са прикачени към компютъра или се намират в близост до него.
- Преценете дали е удачно да попитате потребителя за настройките на системата му, включително пароли, ако обстоятелствата го налагат. Ако Ви бъдат дадени такива данни, бъдете прецизни при записването им.
- Направете подробни записки относно всички предприети действия, свързани с компютърното оборудване.

При откриване на компютърно оборудване, което изглежда включено:

- Обезопасете зоната, в която се намира оборудването.
- Изведете хората далече от компютъра и от източника на захранване.
- Направете снимки или видеоклип на помещението и на всички компоненти в рамките на обекта, включително захранващите кабели. Ако не разполагате с фотоапарат, начертайте план-скица на системата и поставете етикети на портовете и кабелите, за да можете да възстановите системата/системите на по-късен етап.
- Преценете дали е удачно да попитате потребителя за настройките на системата му, включително пароли, ако обстоятелствата го налагат. Ако Ви бъдат дадени такива данни, бъдете прецизни при записването им.
- Запишете какво е изобразено на екрана като направите снимка

или като си запишете какво е съдържанието на екрана.
- Не докосвайте клавиатурата и не натискайте мишката. Ако екранът е черен или ако има включен скрийнсейвър, попитайте длъжностното лице, отговарящо за случая, дали иска да възстановите екрана. Ако това е така, всяко кратко придвижване на мишката би трябвало да доведе до възстановяване на екрана или до показване на скрийнсейвъра, ако той е защитен с парола. Ако екранът бъде възстановен, направете снимка или видеоклип и си запишете какво е съдържал той. Ако се покаже искане за въвеждане на парола, продължете както е описано по-долу, без да пипате мишката повече. Запишете часа и дейността при използване на мишката при такива обстоятелства.
- Когато е възможно, съберете данни, които иначе биха били загубени след разкачване на захранването, например стартирани процеси и информация относно състоянието на мрежовите портове в съответния момент. Уверете се, че за извършените действия направените по системата промени са разбрани и регистрирани.
- Вземайте предвид получени от собственика/потребителя на компютъра съвети, но се уверете, че към получената информация се подхожда предпазливо.
- Дайте възможност на принтерите да завършат разпечатването.
- Ако нямате достъп до съвети от специалист, изключете захранването от задната част на компютъра, без да затваряте никакви програми. Когато разкачате захранването, винаги го правете от страната на компютъра, а не от тази, свързана към контакта. Така ще избегнете записването на данни върху харддиска, ако машината е оборудвана с непрекъсваем захранващ блок (UPS).
- Разкачете всички други свързани кабели, водещи от компютъра към контакти/куплунги на стената или пода, или към други устройства.
- Уверете се, че всички елементи са с подписани и попълнени етикети, прикачени към тях. Ако не направите това, можете да създадете трудности с приемствеността и в резултат от това оборудването да бъде отхвърлено за целите на съдебните експерти.
- Дайте възможност на оборудването да се охлади преди изземването му.
- Претърсете мястото за дневници, тетрадки или листове хартия с пароли – такива често са прикачени към компютъра или се намират в близост до него.
- Направете подробни записки относно всички предприети действия, свързани с компютърното оборудване.

Какво следва да се изземе

За извличане на доказателства (примери):

- Основно устройство: обикновено това е кутията, към която са свързани мониторът и клавиатурата.
- Монитор, клавиатура и мишка (това е необходимо само в някои случаи; ако имате колебания, потърсете съвет от експерт).
- Захранващи кабели (отново, това е необходимо само в някои случаи; ако имате колебания, потърсете съвет от експерт).

- Захранващи блокове.
- Харддискове, които не се помещават вътре в кутията на компютъра.
- Донгъли (вж. речника).
- Модеми (някои съдържат телефонни номера).
- Външни дискове и други външни устройства.
- Безжични мрежови карти (вж. речника).
- Модеми.
- Рутери.
- Цифрови камери.
- Дискети.
- Ленти с резервни копия.
- Jaz/Zip касети.
- компактдискове.
- DVD дискове.
- PCMCIA карти (вж. речника).
- Флашки, карти памет и всички устройства, свързани към USB портове.

Заб.: винаги поставяйте етикети върху пликовете, в които слагате тези артикули, а не върху самите тях.

Ако захранването бъде махнато от работеща система, всички доказателства, съхранявани в криптирани дялове ще бъдат загубени, освен ако не бъде получен достъп до съответния ключ. Също така, обърнете внимание, че потенциално ценни живи данни ще бъдат загубени, което може да доведе до искове за щети, например корпоративни данни.

За подпомагане на прегледа на оборудването, следва да изземете:

- Ръководства за компютъра и софтуера.
- Всичко, което може да съдържа парола.
- Ключове за криптиране.
- Ключове за сигурност – необходими за физическо отваряне на компютърното оборудване и кутиите за съхранение на носители на данни.

За сравнения на разпечатки, следва да изземете:

- Принтери, разпечатки, принтерна хартия за съдебномедицинска експертиза, ако е необходимо.

Други средства за съхранение на данни

Следва да се има предвид, че има различни електронни устройства, които можете да срещнете по време на претърсване, които да съдържат доказателства, свързани с наказателното разследване. Те включват:

- Мобилни телефони.
- Пейджъри.

- Стационарни телефони.
- Телефонни секретари.
- Факс апарати.
- Диктофони.
- Цифрови фотоапарати.
- Цифрови телевизори, способни на достъп до интернет.
- Медийни компютри/сървъри.
- Сателитни приемници.
- Устройства за запис с висока дефиниция.
- Конзоли за игри от следващо поколение.

Ако някой от тези артикули може да бъде иззет и изключен от захранването, неговата памет може да бъде изтрита. Потърсете съвет от експерт преди да предприемете каквито и да било действия.

Транспорт

Основно устройство

Работете внимателно, ако го поставяте в автомобил, го поставете изправено и на място, където няма да бъде изложено на значителни физически сътресения. Дръжте го далече от магнитни източници (високоговорители, отопляеми седалки и прозорци, и полицейски радиостанции).

Монитори

Най-добре е да се транспортират с екрана надолу, на задната седалка на кола, затегнати с колан.

Харддискове

Както при основните устройства, защитавайте от магнитни полета. Поставяйте в антистатични пликове или в здрави хартиени пликове или увивайте в хартия и поставяйте в омекотени пластмасови пликове.

Флашки и PCMCIA карти

Както при основните устройства, защитавайте от магнитни полета. Не прегъвайте или огъвайте. Не поставяйте етикети директно върху дискети.

Лични цифрови органайзери, електронни органайзери и джобни компютри

Защитавайте от магнитни полета.

Клавиатури, захранващи кабели, мишки и модеми

Поставете в пластмасов плик. Не поставяйте под тежки предмети.

Други съображения

- Съхраняване на оборудването за снемане на ДНК и пръстови отпечатъци.
- Ако е вероятно да бъде извършено снемане на пръстови отпечатъци или на ДНК, винаги се консултирайте с длъжностното лице, отговарящо за случая.
- Използването на алуминиев прах върху електронни устройства може да бъде опасно и да доведе до загуба на доказателствата. Преди да използвате подобна субстанция, внимателно преценете с какви опции разполагате.
- Съхранявайте оборудването в условия с нормална влажност и температура на въздуха. Не съхранявайте в условия с прекомерна топлина, студ, влага или влажност.

Батерии

Повечето компютри са в състояние да съхраняват вътрешни данни, включително настройки в CMOS-чип (вж. речника), с помощта на батерии. Батериите трябва да се проверяват на регулярни интервали, за да се запазят доказателствата, до момента, в който всички проверки са завършени и данните са обезопасени. Не е възможно да се определи продължителността на живота на никой вид батерия. Въпреки това е важно да имате предвид когато съхранявате един компютър много дълго време преди извършване на съдебна експертиза и това следва да бъде решено в местната политика за съхранението.

Съхранение след изземване

Компютърното оборудване следва да се съхранява при нормална стайна температура, без да се подлага на екстремна влага и без магнитно въздействие, като например такова от радиоприемници. Някои компютри са в състояние да съхраняват вътрешни данни посредством батерии. Ако се допусне изразходване на батерията, вътрешните данни ще бъдат загубени. Прахът, пушекът, пясъкът, водата и маслата са вредни за компютрите. Алуминиевият прах за снемане на пръстови отпечатъци е особено вреден и опасен.

Местопрестъпления и интернет

Интернет е среда, в която материали могат да се съхраняват, предават или споделят. Въпреки своята големина и сложност, той не е нищо повече от голяма компютърна мрежа. В крайна сметка, всяка информация в интернет физически пребивава върху една или повече компютърни системи и следователно би могла да се извлече чрез съдебна компютърно-техническа експертиза на въпросните физически устройства. Въпреки това, част от информацията лесно може да бъде променена, например съдържанието на директни съобщения между потребители; или може да бъде променена или изтрита преди да бъдат локализирани и прегледани тези устройства, например съдържанието на уебсайт. В такива случаи, може да е необходимо да се съберат доказателства директно от интернет, вероятно по време

на общуване „на живо" със заподозряно лице или чрез записване на живо съдържание на уебсайт.

Имейл (електронна поща)

Имейлите могат да се извлекат за съдебни цели от физически машини, въпреки че при определени обстоятелства може да е необходимо извличане и преглеждане на много малък брой имейли. Разследващите могат да поискат да ги получат от компютърната система на дадена жертва/заподозрян, без да се налага да се съобразяват с евентуалното забавяне за получаване на компютърно-техническата експертиза или без да причиняват значително неудобство на жертвата. При такива обстоятелства, разпечатани копия на самите имейли, включително информация от заглавието, биха били достатъчно доказателство за изпращането/получаването и съдържанието на имейла. Информацията от заглавието обикновено не е видима за получателя, но може да се види чрез програмата на потребителя за получаване и изпращане на имейли (имейл клиент). Заглавната част съдържа подробна информация относно подателя, получателя, съдържанието и датата на съобщението. Разследващите следва да се консултират със служителите в рамките на своите „звена за разследване на компютърни престъпления", ако имат някакви съмнения за това как да извлекат или да тълкуват информацията от заглавната част. Ясно е, че подобна важна информация трябва да се извлича по конвенционален начин, т.е. с установена верига за приемственост като подпис и дата.

Информация за профил – имейл/уебмейл/IP-адрес

Разследващите, които търсят информация за абонати, свързана с имейл, уебмейл или интернет връзки следва да се консултират със специалист от своето звено, който да ги посъветва относно информацията относно абонамента. Всяко искане за телекомуникационни данни подлежи на разпоредбите на съответното законодателство относно защитата на данните.

Уебсайтове/публикации във форуми/блогове

Доказателства, свързани с дадено престъпление могат да се намират върху уебсайт, публикации във форум или онлайн блог. Улавянето на тези доказателства може да създаде някои сериозни предизвикателства, тъй като целевата машина (машини) може да се намира извън съответната юрисдикция, а самите доказателства лесно биха могли да се променят или изтрият. В такива случаи, времето е критичен фактор за извличането на наличните доказателства и разследващите могат да прибягнат до заснемане на екрана докато показва час и дата на съответния материал, или да „копират" цялото съдържание на конкретен уебсайт. Когато се разглежда материал в интернет, с намерение да се ползва за запазване на доказателства, разследващите трябва да използват анонимизиращи системи или услуги. Съвети относно купуването и използването на такива системи следва да се получат от съответните специализирани звена на правоприлагащите

органи. Ако не се използват подходящи системи, това може да доведе до компрометиране на сегашната и бъдещи операции. Разследващите следва да се консултират със съответните специализирани звена, ако искат да „копират" и запазят съдържанието на цял уебсайт.

Разузнаване чрез открити източници

Много от правоохранителните и правоприлагащите органи активно се занимават с проактивни опити за мониторинг на интернет и за откриване на незаконни дейности. В някои случаи мониторингът може да прерасне до „наблюдение" – специално разузнавателно средство (СРС). При такива обстоятелства, разследващите следва да се обръщат към съответните органи на властта, защото в противен случай всички събрани доказателства може впоследствие да бъдат обявени за недопустими. Още веднъж, когато осъществяват такива дейности, разследващите следва да използват анонимизиращи системи и услуги, които не би трябвало да разкрият обстоятелството, че правоприлагащите органи разследват този конкретен дял от интернет.

Работа с метаданни в документите[26]

Метаданните могат да бъдат в два формата: метаданни от приложения и системни метаданни. Метаданните от приложения обикновено се вграждат в документа, така че те „пътуват" с файла при неговото копиране или изпращане по имейл. Тази форма на метаданни се генерира като функция на дадено приложение, което е използвано за създаването на даден файл, и инструктира това приложение по какъв начин да показва даден документ на екрана. Документът действително съхранява, до различна степен, информация относно жизнения цикъл на документа, от създаването му до унищожаването му.

Документите, създадени с програми от пакета Microsoft Office, като например Word и Excel, могат да съдържат изключително ценни метаданни от приложението.

Метаданните в документите на Microsoft Office обикновено се създават автоматично и без знанието на потребителите, включително:

- Автор, длъжност, тема, ключови думи, фирма и коментари
- Дата на създаване, дата и час на последен запис, дата и час на последно разпечатване, запазен от, номер на ревизия, общо време на редактиране

В документите от Microsoft Office могат да се съдържат още няколко други вида скрита и лична информация:

- Коментари и редакционни бележки от функцията на Microsoft Word за проследяване на промените: Съдебният експерт може да използва тази функция, за да установи въведени промени в

[26] За основа служи документът: *Нарастващата роля на технологиите в усилията за борба срещу измамите*, JEAN-FRANÇOIS LEGAULT, Асоциация на сертифицираните експерти по измамите, 2011.

документите с течение на времето и да види имената на потребителите, които са работили върху него и са ги преглеждали когато тази функция е използвана от съответните лица за редактиране на документа. Представете си случай, при който подозирате, че някои доставчици са фалшифицирали тръжни оферти. В едно от предложенията, записано като документ в Microsoft Word, успявате да възстановите изтрит коментар, чрез функцията за проследяване на промените, който е направен от шефа на доставчика: „Променете цената на 500 000 евро; другите са съгласни."

- Скрит текст и скрити данни: текстът в документите в Microsoft Word и редовете и колоните в Microsoft Excel могат да се форматират като „скрити", за да не се разпечатват. Въпреки това, проверяващият експерт може да види информацията, която се съдържа в оригиналния електронен документ.
- Вградени елементи: документите могат да съдържат вградени графики и текст, генерирани с други програми. Например, една таблица в документ в Microsoft Word за финансов отчет може на практика да съдържа електронна таблица от Microsoft Excel. Проверяващият експерт може да успее да види .XLS файла, от който тази таблица е взета и да провери изчисленията, които са използвани за генериране на информацията, представена в .DOC документа.

Разследващите могат да открият файлове във формат за документи на Adobe (.PDF), които на практика са документи от Microsoft Office, които са конвертирани в този формат. От тях могат да бъдат извлечени метаданните, които идентифицират автора на документа (лицето, което го е конвертирало), датата и часа на създаване (датата, на която е конвертиран), името на оригиналния документ и софтуера, който е използван за създаване на .PDF документа.

Формат Exif – това е спецификация за файлов формат на изображения, който се използва от цифрови фотоапарати. Той взема за основа съществуващия JPEG формат, който се използва от повечето цифрови фотоапарати, но съдържа допълнителни маркери с метаданни, които включват:

- Производител и модел
- Дата и час на създаване на снимката
- Време на експозиция, апретура, дали е използвана светкавица, ISO еквивалент

Съвременните фотоапарати и смартфони съхраняват координати от глобалната система за позициониране (GPS) под формата на Exif маркери в метаданните на JPEG формата. Тази информация, известна като геолокация, може да бъде изключително полезна за установяване на мястото, където конкретни събития са се случили.

За разлика от метаданните от приложения, които се вграждат в описания файл, системните метаданни се съхраняват извън тях, върху организационна система. Това включва елементи като името на файла; неговото местоположение в системата; неговият размер; по-

требителят, който е създал файла; и датите на създаване, изменение и достъп.

Метаданните от приложение и системните метаданни са два различни източника, които могат да носят различна информация. Например метаданните от приложението показват, че авторът на документа е „Иван Иванов", но системните метаданни показват, че документът е създаден от „Иван Петров". Едно възможно обяснение: „Иван Иванов" може да е автор на документа на един компютър и след това да го е изпратил на „Иван Петров" по имейл, който след това го е запазил на своя компютър. В резултат на това, авторът на документа продължава да бъде „Иван Иванов", но лицето, което го е създало върху съответната система е „Иван Петров".

ПРИЛОЖЕНИЕ 2. РЕЧНИК И ОБЯСНЕНИЕ НА ТЕРМИНИТЕ

АДРЕС

Терминът „адрес" има няколко различни приложения:

- Интернет адрес или IP-адрес (IP = интернет протокол) представлява уникалното местоположение на даден компютър в интернет.
- Адресът на уеб страница се изразява като дефиниран път сред директориите до конкретен файл, намиращ се върху съответния сървър.
- Адресът на уеб страница се нарича също URL (унифициран локатор на ресурси).
- Имейл адресът представлява местоположението на конкретен потребител на електронна поща (изразява се чрез имейл името на потребителя, последвано от знака „@", последван от името на домейна, зачислен на сървъра, върху който се помещава имейл адресът)

АРХИВЕН ФАЙЛ

Файл, който съдържа други файлове (обикновено в компресиран вид). Той се използва за съхранение на файлове, които не се използват често или файлове, които потребителите на интернет могат да изтеглят от библиотека с файлове.

BIOS

Basic Input Output System (основна входно-изходна система). Програма, която се съхранява върху дънната платка и контролира взаимодействието между отделните компоненти на компютъра.

ДИСК ЗА ЗАРЕЖДАНЕ

Отнася се за диск, който съдържа файловете, необходими за стартиране на операционна система.

CMOS чип

Допълнителен полупроводник на основата на метален окис. Този чип обикновено служи за съхранение на настройките на BIOS системата при изключване на захранването, с помощта на батерия.

CRC проверка

Циклична проверка на повторенията. Това е широко разпространена техника за откриване на грешки при предаването на данни.

КРИПТОГРАФИЯ

Процесът на обезпечаване на сигурността на лична информация, която се изпраща през обществени мрежи, чрез нейното криптиране по такъв начин, че тя да бъде нечетима за всички останали, освен лицето или лицата, които разполагат с математическия ключ/познания как да декриптират информацията.

БАЗА ДАННИ

Структурираното събиране на данни може да се извърши по много начини. Някои от най-разпространените програми за бази данни са: Dbase, Paradox, Access. Форми на ползване: разнообразни, включително – препратки към адреси, информация за фактуриране и др.

ИЗТРИТИ ФАЙЛОВЕ

Ако даден субект знае, че има уличаващи файлове на компютъра, той може да ги изтрие, за да се опита да заличи доказателствата. Много потребители на компютри си мислят, че с това информацията действително се заличава. Въпреки това, в зависимост от начина, по който е извършено изтриването на файловете, в много случаи съдебен експерт ще може да възстанови оригиналните данни – частично или изцяло.

ЦИФРОВ ПОДПИС

Използване на криптография за осигуряване на автентификация на съответните входящи данни, или съобщение.

ДОНГЪЛ

Термин за малко външно хардуерно устройство, което се свързва с компютъра, за да осигури автентификация на конкретен софтуер; например, доказателство, че даден компютър действително разполага с лиценз за използвания софтуер.

КРИПТИРАНЕ

Процесът на разбъркване или кодиране на информацията, за да се гарантира, че само целевият получател ще може да я прочете.

ЗАГЛАВИЕ/ЗАГЛАВНА ЧАСТ НА ИМЕЙЛ

Имейлите (електронните писма) имат две части – основна част и заглавна част. Обикновено заглавната част дава на получателя информация относно часа, датата, подателя и темата. Всички имейли имат и (обикновено скрита) разширена заглавна част – информация, която се добавя от програмите за електронна поща и изпращащите устройства – която показва допълнителна информация относно подателя, която в много случаи може да се проследи до конкретен компютър в интернет.

СВОБОДНО ПРОСТРАНСТВО

Файлови клъстери, които към момента не се използват за съхранение на „живи" файлове, но могат да съдържат данни, които са „изтрити" от операционната система. В такива случаи е възможно възстановяване на цели файлове или на част от тях, освен ако потребителят не е използвал специализиран софтуер за почистване на дисковото пространство.

ХОСТ СИСТЕМА

За целите на настоящия документ, хост системата е такава, която се използва за приемане на харддиск от друг компютър, за целите на съдебно разследване.

ХЪБ

Централно свързващо звено за всички компютри в дадена мрежа, обикновено базирано на Ethernet-протокола. Информацията, която се изпраща до хъба може да достигне до всеки друг компютър в мрежата.

IMEI номер

Международен идентификатор на мобилно оборудване. Уникален 15-цифров номер, който служи като сериен номер на даден GSM апарат.

IMSI номер

Международен идентификатор на мобилен абонат. Уникален за целия свят кодов номер, чрез който се идентифицира абонатът на дадена мрежа, на който е зачислен конкретен GSM апарат.

LINUX

Операционна система, която е популярна сред ентусиастите и за някои приложения в бизнеса.

МАГНИТЕН НОСИТЕЛ НА ДАННИ

Диск, лента, касета или дискета, използвани за магнитно съхранение на данни.

ПАМЕТ

Често се използва като по-кратко название за оперативната памет (RAM). Паметта представлява временно електронно хранилище за инструкции и данни, до които микропроцесорът на компютъра има скоростен достъп. RAM-паметта се намира върху един или повече микрочипове, инсталирани в даден компютър.

MS-DOS

Дискова операционна система на Microsoft. Някога това беше най-разпространената операционна система при настолните персонални компютри. Автоматично се зарежда в паметта на компютъра и работи до изключването му. Често се нарича просто DOS.

ORB

Система със сменяеми харддискове с висок капацитет. ORB-устройствата използват технология с магниторезистивна (MR) четяща/записваща глава.

PCMCIA КАРТИ

Подобни по размер на кредитните карти, но по-дебели от тях. Тези карти се поставят в слотовете на даден лаптоп или джобен компютър и осигуряват много функции, които обикновено не са налични за машината (модеми, адаптери, харддискове и др.)

ПОРТ

Думата „порт" има три значения:

- Когато информацията влиза в даден компютър или излиза от него, например сериен порт на персонален компютър, в който може да се включи модем.
- По отношение на протоколите TCP и UDP, свързани с работата на компютър в мрежа, портът представлява номер, който присъства в заглавната част на пакет с данни.

Портовете обикновено се използват за картографиране на данни към конкретен процес, който се изпълнява от даден компютър. Например, порт 25 обикновено се използва с протокола SMTP, порт 80 – с HTTP, а порт 445 – с HTTPS.

- „Порт" може също да се отнася за превеждането на част от софтуер, за да може той да се използва на друг тип компютърна система, например за превеждане на програма за Windows, така че тя да може да работи на компютър с Macintosh система.

СОФТУЕР В ПУБЛИЧНИЯ ДОМЕЙН

Всяка програма, която не е защитена с авторски права.

PUK код

Личен ключ за разблокиране. PUK кодът служи за разблокиране на SIM картата на даден GSM апарат, която е била блокирана след въвеждане на грешен PIN код три пъти подред.

RAM памет

Памет с произволен достъп – краткосрочната работна памет на даден компютър. Тя осигурява работно пространство за компютъра, така че той да може да работи с данни с висока скорост. Информацията, която се съхранява в RAM паметта се губи при изключване на компютъра („променливи данни").

СМЕНЯЕМИ НОСИТЕЛИ НА ДАННИ

Това са дискети, компактдискове, DVD-дискове, касети и др., които служат за съхранение на данни и могат лесно да се сменят.

ШЕЪРУЕР

Софтуер, който се разпространява безплатно като пробна версия, с разбирането, че ако се използва след изтичането на пробния период, потребителят ще трябва да заплати за него. Някои версии на шеъруер са програмирани с вградена дата на изтичане.

СМАРТ-КАРТА

Пластмасови карти, обикновено с вграден електронен чип, които съдържат токен с определена електронна стойност. Тази стойност може да се използва както за физически търговски обекти, така и за онлайн магазини.

СУИЧ

Обикновено малка, плоска кутийка с 4 до 8 Ethernet порта. Тези портове могат да служат за свързване на компютри, кабелни или DSL модеми и други суичове. Суичът насочва мрежовите комуникации между конкретни системи в мрежата, за разлика от други устройства, които могат да излъчват информацията до всички звена от мрежата.

СИСТЕМЕН БЛОК

Обикновено най-голямата част от персоналния компютър, системният блок представлява кутия, в която се помещават основните компоненти. Обикновено устройствата са разположени отпред, а портовете за свързване на клавиатура, мишка, принтер и други устройства – отзад.

UNIX

Много популярна операционна система. Използва се предимно върху по-големи системи, позволяващи едновременен достъп на множество потребители.

USB УСТРОЙСТВА ЗА СЪХРАНЕНИЕ

Малки устройства за съхранение, достъпни чрез USB портовете на компютъра, които позволяват съхранението на големи обеми от файлове с данни и които лесно могат да се махат, транспортират и крият. Размерът им е приблизително колкото ключ за кола или текст-маркер; могат дори да се носят около врата като накит. В днешно време съществуват най-различни формати – могат да изглеждат като нещо съвсем различно, например часовник или швейцарско ножче.

USIM

Подобрена версия на Модул за идентификация на абоната (SIM-карта), проектирана за използване на третата генерация (3G) мрежи.

ВИРТУАЛНА ПАМЕТ

Място за съхранение в интернет, предлагано от трета страна, което позволява съхраняване и извличане на данни чрез който и да било браузър. Примери за такава услуга са: GDrive, One Drive, DropBox и др.

БЕЗЖИЧНА МРЕЖОВА КАРТА

Разширителна карта, която се поставя в компютъра и позволява безжична връзка между съответната машина и други устройства в съответната компютърна мрежа. Тя замества традиционните мрежови кабели. Картата използва радиосигнали за своята комуникация с други устройства в мрежата.

ZIP устройство/ZIP диск

Модифициран защитен формат на устройство със сменяеми 3.5-инчови дискове, произвеждано от Iomega. Устройството се предлага в пакет със софтуер, който може да създава каталози на дисковете и да заключва файлове от съображения за сигурност.

ZIP

Популярен формат за компресиране на данни. Файловете, които са компресирани в ZIP формат, се наричат ZIP файлове и обикновено са с разширение .ZIP.

ПУБЛИКАЦИИ НА ЦЕНТЪРА ЗА ИЗСЛЕДВАНЕ НА ДЕМОКРАЦИЯТА

Антикорупция: прилагане и оценка на антикорупционни мерки и политики (МАКПИ), С., 2017.
ISBN: 978-954-477-312-0

Трансгранична организирана престъпност: България и Норвегия в контекста на миграционната криза, С., 2017.
ISBN: 978-954-477-318-2

Мониторинг на рисковете от радикализация, С., 2017.
ISBN: 978-954-477-300-7

Ситуационна оценка на тенденциите в екстремизма, С., 2017.
ISBN: 978-954-477-296-3

Корупцията в частния сектор в България, С., 2017.
ISBN: 978-954-477-329-8

Изнудването и рекета в ЕС: фактори за уязвимост, С., 2016.

Завладяване на държавата: противодействие на административната и политическата корупция, С., 2016.
ISBN: 978-954-477-277-2

Мониторинг на антикорупцията в Европа, С., 2015.
ISBN: 978-954-477-241-3

CSD Policy Brief No. 56: Динамика на конвенционалната престъпност 2014 – 2015 г., С., 2015.

CSD Policy Brief No. 50: Финансирането на организираната престъпност: институционални мерки за противодействие, С., 2015.

CSD Policy Brief No. 48: Антикорупционни мерки в правоохранителните институции, С., 2015.

Financing of organised crime (на английски), С., 2015.
ISBN: 978-954-477-234-5

Заплахите за финансовите интереси на Европейския съюз: оценка на риска от злоупотреби при обществените поръчки използването на европейските фондове, С., 2013.
ISBN: 978-954-477-212-3

Оценка на заплахите от тежката и организираната престъпност 2010 – 2011, С., 2012.
ISBN: 978-954-477-186-7

Организираната престъпност в България: пазари и тенденции, С., 2007.
ISBN: 978-954-477-151-5