МЕТОДИ И СРЕДСТВА ЗА ПОВИШАВАНЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ НА ОБЛАЧНИТЕ ИЗЧИСЛЕНИЯ В ПРАКТИКАТА НА МАЛКИТЕ И СРЕДНИТЕ ПРЕДПРИЯТИЯ

Ас. Ангелин Лалев

Резюме: Настоящата статия разглежда проблемите на информационната сигурност при облачните изчисления от гледна точка на малките и средните предприятия (МСП) и ограниченията, които тези предприятия имат по отношение на информационните технологии. В разработката се обсъждат организационни и технически мерки за защита, които са сравнително лесни и достатъчно евтини, за да могат да бъдат приложени от МСП по отношение на заплахите за информационната сигурност в облачна среда.

Ключови думи: информационна сигурност, малки и средни предприятия, облачни изчисления.

JEL: C88, C89.

По отношение на информационната сигурност, както по принцип, така и вчастност за облачните изчисления, МСП формират особена група организации. Те са изключително разнородни по своята същност, което намира израз и в драстично различните нужди от информационна сигурност, които има

всяко отделно МСП. Общото между по-голямата част от МСП обаче са две важни особености, които ги отграничават от много други категории стопански и нестопански организации. **На първо място**, МСП обикновено разполагат със силно ограничени бюджети за информационни технологии. **На второ място**, МСП рядко разполагат с достатъчно специализиран в областта на информационната сигурност персонал.

Тези две ограничения възпрепятстват постигането на адекватна информационна сигурност и правят МСП удобна цел за атаки. Това се потвърждава от наблюдения в практиката, където през последните 5 години ставаме свидетели на масови атаки, насочени специфично към МСП и особено към техните електронни магазини. Тези атаки типично обхващат хиляди МСП (а в някои рекордни случаи – стотици хиляди МСП), а целта им е придобиване на достъп до банкови и картови данни, които да послужат за директна кражба на средства *(Constantin, 2016), (Bad bytes Security Blog, 2011)*.

Един аспект на информационната сигурност на МСП, засегнат в най-сериозна степен от споменатите ограничения, касае облачните изчисления. Те са привлекателни за МСП поради значителните икономии на средства, до които води изнасянето на обработката на данни към облачните доставчици. Внедряването им обаче изменя информационната среда, в която функционира организацията. Този процес крие множество нови проблеми и предизвикателства за информационната сигурност на МСП.

Настоящата публикация има за цел формулирането на мерки за повишаване на информационната сигурност на облачните изчисления в МСП, които са групирани в две направления – организационни и технически. Организационните касаят дейности като определяне на данните, които са изложени на риск, и оформяне на правилата на организацията за работа с данните. Техническите мерки касаят настройките и конфигурирането на софтуера и хардуера на информационните системи.

1. Заплахи за облачните изчисления в практиката на МСП

Формулирането на мерки за защита на информацията и анализ на риска не може да бъде извършено адекватно, ако то не се основава на добро разбиране за заплахите, които съществуват по отношение на информационната сигурност в облаците. Въпросът, кои са тези специфични за облачните изчисления заплахи, е свързан с редица условности.

Много важен факт, който трябва да се има предвид при формулирането на различните категории заплахи за облачните изчисления, е това, че всъщност под самото понятие „облачни изчислния“ се разбира доста разнороден кръг от услуги. Различните видове облачни услуги са изложени на различен набор от заплахи, но по-съществената разлика между тях е свързана с това, че различните модели на услугата разпределят по различен начин отговорностите по осигуряване информационната сигурност между организацията и облачния доставчик. В този смисъл при един модел на услугата дадени заплахи са отговорност на облачния доставчик, докато при друг модел те са съответно отговорност на организацията.

Между гъвкавостта на облачните услуги и количеството дейности по информационната сигурност, делегирани на облачния доставчик, има обратнопропорционална връзка. IaaS услугите предлагат най-голяма гъвкавост и се радват на най-голяма популярност, но те в най-малка степен делегират дейностите по информационната сигурност на доставчиците. (вж. табл. 1).

Приблизителната връзка между дейностите, описани в Таблица 1, и евентуалните заплахи, адресирани от тези но, че изборът на PaaS или IaaS услуги все още изисква, предприятието да внедрява технически мерки за справяне с много сериозни потенциални заплахи за сигурността, докато SaaS услугите по-скоро изискват прилагане на организационни мерки.

Таблица 1.
Отговорности на клиента на облачни услуги по отношение на основни повтарящи се дейности за осигуряване на информационна сигурност

	Обновяване на ОС	**Обновяване на приложния софтуер**	**Конфигуриране на мрежови услуги**	**Конфигуриране на защитните стени**
SaaS[1]	Не	Не	Не	Не
PaaS[2]	Не	Да	Частично	Не
IaaS[3]	Да	Да	Да	Да

Таблица 2.
Заплахи за информационната сигурност, адресирани от дейностите в Таблица 1

Дейност/ Мярка	**Най-чести заплахи, свързани с неправилното или непълно провеждане на дейността / мярката**	**Ефект**	**Риск**
Обновяване на ОС	Вируси, червеи, „експлойти“, кражба и подмяна на информация.	Установяване на пълен контрол над атакуваните сървъри.	Директни кражби на средства. Издаване на документи с фалшиво съдържание. Кражба на лични данни. Невъзможност за лесно откриване на източника на пробива. Голям престой при отстраняване на проблема.
Обновяване на приложния софтуер	Вируси, червеи, „експлойти“, кражба и подмяна на информация. Предпоставки за провеждане на атаки срещу операционната система.	Установяване на частичен контрол над атакуваните сървъри.	Директни кражби на средства. Издаване на документи с фалшиво съдържание. Кражба на лични данни.
Конфигуриране на мрежови услуги	Кражба и подмяна на информация.	Предпоставки за провеждане на атаки срещу приложния софтуер.	Кражба на лични данни. Директни кражби на средства.
Конфигуриране на защитните стени		Предпоставки за провеждане на атаки срещу мрежовите услуги.	Престой, косвени ефекти.

[1] От англ. „Software as a Service” – софтуер като услуга.
[2] От англ. „Platform as a Service” – платформа като услуга.
[3] От англ. „Infrastructure as a Service” – инфраструктура като услуга.

Освен изброените по-горе заплахи, които могат да се определят като „универсални“ и засягат почти всяка свързана към мрежата компютърна система, облачната среда представя свои уникални предизвикателства към сигурността, които трябва да бъдат адресирани. Някои от най-важните са:

- използването на облачни услуги включва нови субекти в дейностите по осигуряване на сигурността. Това са облачните доставчици, чиито пропуски, отношение и добронамереност стават решаващ фактор за сигурността, тъй като по необходимост облачният доставчик има пълен достъп до данните на организацията в облака. По тази причина делегирането на обработката на данни повдига не само технически, но и правни въпроси.

Важен казус в това отношение е обезсилването от Европейския съд на договора U.S.-EU Safe Harbour Act през 2015 г. Той уреждаше юрисдикцията върху данните на фирми от ЕС, когато те се намират физически на сървъри, разположени на територията на САЩ. Договорът бе отменен от съда на основание на това, че не предлага адекватна правна защита на личните данни на гражданите на ЕС. Неговото отпадане демонстрира, че, невъзможността да бъдат защитени адекватно данните срещу злонамерени дейности от страна на самия облачен доставчик, може да доведе до забрани за прехвърляне на определени категории данни (например лични данни) в облаците (Meyer, 2016). За МСП подобни перспективи се транслират в риск, тъй като подобни развития имат капацитета да засегнат сериозно информационната инфраструктура на МСП и неговото присъствие в Интернет, при условие че то използва облачни изчисления в своята дейност. Причините за това са следните:

- облачните услуги по необходимост „отварят“ ИТ инфраструктурата на организацията към Интернет, елиминирайки част от полезността на защитните стени и правейки сигурността на инфраструктурата много по-зависима от криптографски мерки. Прилагането на криптографски мерки никога не е

тривиална задача поради постоянната еволюция на тази материя, която поначало изисква много сериозни знания и умения за правилно прилагане;

- облачните услуги (и особено публичните SaaS услуги като Gmail, Drive и т.н.) провокират използването на информацията от домашни компютри и мобилни устройства, което може да е особено негативно за сигурността на чувствителната информация.

Описаните особености подсказват къде следва да се насочи оценката на риска в МСП, както и последващите мерки за защита. Всяко предприятие обаче следва индивидуално да прецени как описаните по-горе заплахи се проектират върху информационната среда, в която действа предприятието.

2. Оценка на риска в МСП

Както бе споменато, проблемите при МСП по отношение на определянето на това кои данни се нуждаят от допълнителна защита, са по своята същност методологически. Повечето предприятия в тази категория нямат нужното ноу-хау, време и ресурси за провеждането на подробни анализи. Освен това подобни предприятия рядко имат опит с измерването и оценяването на рискове от всякакъв тип. Поради това изключително полезно за тях би било формулирането на набор от методи, които са достатъчно лесни за реализиране в подобна среда. Измежду многото методи за оценка на риска изпъкват два, които отговарят на горепосочените условия.

Бизнес-импакт анализът е общ метод, който е подходящ за прилагане от организации със сравнително ниска култура и ноу-хау в областта на информационната сигурност. Неговите принципи са дефинирани в ISO 22301 и ISO 22313. Методът се използва за формално оценяване на щетите от прекъсванията на дейността на предприятието.

Бизнес-импакт анализът има много разновидности, но винаги се опира на идентифицирането на критичните за бизнеса на предприятието дейности и определянето на максималните периоди, за които тези дейности могат да бъдат прекъснати. Анализът преминава през поредица от стъпки (Wrenn, 2011), измежду които са:

- изготвяне или набавяне на детайлни описания на информационните системи на организацията;
- определяне на критичните за дейността на предприятието дейности чрез анализ на взаимните зависимости между тях; определяне на връзката между информационните системи и критичните дейности чрез определянето на основните заинтересовани лица (в и извън организацията);
- определяне на най-лошите възможни моменти във времето, когато може да бъде прекъсната работата на информационните системи на организацията;
- определяне на нужните ресурси за работата на критичните процеси, включително и тези, свързани с обработката на информация (например персонал, мрежови достъп и т.н.);
- определяне на т.нар. „Recovery Time Objective" или „RTO" – времето, за което по план трябва да се възстанови дейността на критичните бизнес системи;
- определяне на максимално допустимия отрязък назад във времето, за който информацията може да липсва **след като информационните системи са възстановени и възобновят работата си** – "Recovery Point Objective" или „RPO".

Приложени към облачните изчисления, споменатите стъпки улесняват идентифицирането на информацията, която има критично значение за организацията и е потенциално изложена на рискове в облаците.

Бизнес-импакт анализът има и няколко фундаментални ограничения:

- Според стандартите бизнес-импакт анализът е замислен като цялостна процедура, която да оцени готовността на предприятието за справяне с бедствия и аварии от всякакъв вид – т.е. много от предписаните стъпки и принципи в процеса на извършването му не касаят пряко информационните системи на организацията и още по-малко – използването на облачни изчисления;
- Друг, по-сериозен недостатък, е това, че **бизнес-импакт анализът е ориентиран специфично към щетите от *прекъсване* на работата на предприятието и в случая с облачните изчисления – на работата на информационната система.** Освен от прекъсване обаче пробивите в информационната сигурност на организацията обикновено водят и до други ефекти, които са очертани от класическата „CIA триада“ (Schwartau, 2001). **В понятията на CIA триадата бизнес-импакт анализът се концентрира само върху ефектите от нарушаване на наличността на данните. Трябва да се има предвид обаче, че нарушаването на другите два аспекта – поверителност и достоверност, наред със спирането на работата за одит, преинсталиране и възстановяване на данните от архиви, могат да доведат и до много по-тежки последствия и загуби.**

Такива могат да бъдат още:

- директни кражби на средства от банковите сметки на фирмата;
- разочарование у клиентите и евентуалното им напускане;
- глоби, наложени от регулаторни органи;
- пропуснати ползи и конкурентни предимства, включително сключени договори, привлечени потребители.

Размерът на тези щети не е толкова пряко свързан с начина, по който бизнес процесите са организирани и зависят един от друг, така че подходът на бизнес-импакт анализа

трудно може да донесе нова полезна информация за тяхното оценяване.

Методът „Анализ на дървото на грешките“ дава основа както за качествен, така и за количествен анализ. Освен това методът акцентира върху определянето на вероятността за настъпването на даден сценарий, което допълва изложения по-горе метод на бизнес-импакт анализа. Вариация на този метод, разработена през 90-те години (Salter, 1998), е известна като „дърво на атаките“.

Според авторите на метода всяка атака срещу сигурността на една информационна система има три етапа – идентифициране на слабост, придобиване на достъп и изпълнение на атаката. Една система може да бъде окачествена като „слаба“, ако не предоставя достатъчно мерки срещу изпълнението на трите фази на дадената атака.

Дървото на атаките представлява ориентирано дърво. На най-горното ниво (коренът на дървото) се поставя ефектът от материализирането на атаката. Това може да бъде например кражба на информация за клиентите на фирмата или например кражба на средства от банковата сметка на фирмата.

На второ ниво се поставят етапите от жизнения цикъл на информационната система, като например проектиране, разработване, внедряване, изваждане от експлоатация.

На по-долните нива се систематизират заплахите за информационната сигурност на всяко ниво от жизнения цикъл на системата, като се работи дедуктивно. За всеки връх на дървото се изреждат всички известни възможни начини да бъде материализирана описаната заплаха. Така например кражбата на данни за клиентите на фирмата може да се дължи на дистанционната им кражба от информационната система, изнасянето им от вътрешен човек и т.н. На свой ред кражбата от информационната система може да бъде следствие от социално инженерство[4] или следствие от хакерска атака.

[4] Измама, при която цел на атакуващия е да манипулира работещите с информационната система, а не да преодолее техническите мерки за защита.

Отделните ребра в дървото представляват връзки от тип „И“/“ИЛИ“, което отразява как комбинации от фактори могат да предизвикат материализирането на дадена заплаха. Оформеното дърво позволява извършването на прост анализ – избира се дадена запллаха и по ребрата в дървото остава да бъде проследено кои фактори биха довели до евентуалното материализиране на заплахата. Отделно към всеки връх на дървото е възможно да се добавят вероятности, които позволяват изчисляването на общата вероятност за настъпване на дадено събитие.

Основното предимство на метода е ясното излагане на връзките между отделните фактори и заплахи, което е чудесна основа за качествен анализ. Недостатък на метода е, че изчисляването на точни резултати зависи от правилното замерване на вероятностите за материализиране на всеки фактор или заплаха. Последното е трудоемко и на практика може да се извърши само приблизително, което, с натрупването на броя на факторите, би дало драстични отклонения в крайната вероятност.

Двата метода са само представители на сравнително голямо множество от методи и подходи за качествено и количествено оценяване на риска. При наличие на време и желание МСП могат да допълнят анализите си с помоща на повече от 20 метода, описани в ISO 31000. Може да се заключи обаче, че анализите, извършени от МСП, ще бъдат по-неточни и по-приблизителни от тези, които могат да бъдат извършени от по-големи организации, независимо от избраните методи.

3. Мерки за защита на информацията на МСП в облачна среда

С оглед на изложените обстоятелства е съвсем логично да се зададе въпросът съществуват ли мерки, които повишават устойчивостта на облачните изчисления срещу различни по-

тенциални заплахи. В същото време тези мерки не трябва да водят до съществени повтарящи се разходи и да са достатъчно евтини, за да не се налага, употребата им да бъде предмет на прецизни анализи от типа разходи – ползи. Отговорът в много случаи е положителен, с уговорката, че много от тези мерки снижават риска, но до нива, които остават далеч от тези, които са считани за „максимално“ сигурни. Подобни мерки условно могат да бъдат разделени на технически и организационни, тъй като облаците елиминират отговорността на предприятието за физическия аспект на информационната сигурност.

Техническите мерки, които са особено ефективни и в същото време достатъчно евтини и лесни за реализация са:

1) **обновяване на браузърите до последната актуална версия**

Над 99 процента от потребителите в Интернет използват един от петте основни браузъра – Chrome, Edge, Mozilla Firefox, Safari и Opera. Дългогодишната практика до момента показва, че само тези пет големи софтуерни проекта за разработване на браузъри успяват едновременно да поддържат постоянно изменящите се стандарти за уеб технологиите и да извършват бързо отстраняване на откритите грешки. Ако предприятието използва друг мобилен или стационарен софтуер в ролята на браузър, усилията трябва да се насочат към подмяната му с един от посочените браузъри. Особено предизвикателство в тази насока е обновяването на мобилните браузъри. Това често не може да се направи ефективно за стари мобилни телефони и таблети, което налага подмяната им или изработване на политика за достъп, която изключва подобни устройства.

2) **забрана на използването на остарели криптографски протоколи от браузърите и сървърите**

Повечето браузъри имат възможност за допълнителни настройки на сигурността и набора от шифри, използвани от браузъра. Стандартният набор от шифри представлява компромис между възможността за достъп до повечето сайтове в

Интернет и нуждите от сигурност. Повишаването на сигурността чрез изключване на старите набори от шифри ще „счупи“ достъпа до много сайтове в Интернет, но не и до типичните модерни SaaS, PaaS и IaaS услуги. Това може да бъде компенсирано, като се въведе използването на два браузъра в МСП – „стандартен“ и такъв, който е предназначен за достъп до фирмените данни и приложения в облака.

3) активиране на защитните мерки срещу експлоатиране на грешки в софтуера и операционната система

Операционните системи имат допълнителни механизми за защита, които предотвратяват атаки срещу клиентския и сървърния софтуер, както и срещу самата операционна система. Такива са:

- защита от изпълнение на страници с данни;
- защита от дереференции на нулев указател;
- рандомизация на разполагането на адресното пространство;
- откриването и предотвратяването на Heap Spray атаки;
- защитата срещу презаписване на обработчиците на структурирани изключения.

Изброените техники могат да се активират сравнително лесно или директно, или чрез широко достъпни помощни програми. Тази дейност може да се извърши както от страна на сървърите, така и от страна на клиентите. Прилагането на тези мерки обаче може да предотврати работата на приложните програми, тъй като в редки случаи поведението, срещу което мерките са насочени, е част от нормалната работа на напълно легитимна програма. Въпрос на тестване е да се определи има ли програми, които не са съвместими с дадена мярка.

4) активиране на HTTP Strict Transport Security (HSTS) на фирмените сървъри в облака

Активирането на HSTS позволява защита срещу определен клас фундаментални атаки, които премахват криптографската защита напълно от връзката между сървъра и кли-

ента. Правилното внедряване на HSTS изисква, МСП да се ангажира със заплащането на необходимите разходи за електронни сертификати и поддържането на нужната инфраструктура в дългосрочен план, тъй като веднъж активирана, тази мярка остава в сила най-малко година.

5) Активиране на задължителен контрол на достъпа от страна на сървърите

Задължителният контрол на достъпа, за разлика от контрола по преценка, позволява на администратора да зададе правила за защита, които не могат да бъдат отменяни от потребителя –собственик на дадения обект. Тази функция се използва за създаване на своеобразни прецизни профили на всяко приложение, които определят до кои ресурси приложението има достъп.

Много важно значение за МСП имат и редица **организационни мерки**. Тяхното внедряване при МСП всъщност е полесно от това при големите организации и най-общо се състои в мерки за предотвратяване на поставянето на чувствителна информация в облаците на първо място.

1) Използване на Traffic Light Protocol (TLP). TLP дефинира четири нива на поверителност (USCERT, 2017). Те са:

- Червено – информацията, етикетирана като ниво „червено“, не следва да се поделя с никого освен с лицата, от които идва.
- Жълто – информацията, етикетирана като ниво „жълто“, може да се споделя само с ограничен брой служители вътре в организацията, чиито задължения имат пряко отношение към информацията.
- Зелено – информация, която може да се споделя със служители на цялата организация, без да напуска границите на организацията.
- Бяло – информация, която може, свободно да се разпространява в и извън организацията.

От гледна точка на облаците Traffic Light протоколът е изключително удобно средство за обозначаване на информа-

цията, тъй като избраните нива на поверителност кореспондират с проблемите на поделяне на „суверенитета“ върху данните. Така например нивата „червено“ и „жълто“ определено предполагат съхраняването на информацията физически на територията на организацията, докато информацията с ниво „бяло“ е публично достъпна, тоест не е източник на проблеми при съхраняване и обработка в средата на публични облаци.

Traffic Light протоколът е замислен като прост и лесен за разбиране и употреба. Освен това TLP не е обвързан с технически средства за реализация и може да се прилага както към електронни, така и към хартиени документи. Това са и основните му предимства.

Основният недостатък е, че TLP не е обвързан по никакъв начин с електронни средства за реализация и съблюдаването на ограниченията е изцяло отговорност на потребителите. Друго важно ограничение на TLP е, че той може да се прилага много по-лесно към неструктурирани документи, отколкото към структурирана информация и бази от данни.

2) Използване на виртуални стаи за данни. Виртуалните стаи за данни са именувани по аналогия с реалните корпоративни хранилища на документи, в които документите понякога се ползват на място, без да е разрешено тяхното физическо изнасяне от хранилището. Продуктите, които се предлагат като такива виртуални стаи за данни, целят същото с електронните документи. Те ограничават функционалността, достъпна на потребителя до четене на документа, като се опитват да забранят записването, препращането, отпечатването и пр. други дейности върху документа, които биха могли да се използват за кражба на съдържанието му.

Виртуалните стаи за данни имат редица предимства спрямо TLP, главното от което е, че благодарение на избрания подход достъпът до документите се регулира централизирано и автоматично. За облачните изчисления това означава, че виртуалната стая за данни може да предотврати случайното прехвърляне на чувствителна информация в облака.

На свой ред виртуалните стаи за данни имат множество недостатъци. Те предлагат сигурност, базирана на скриване, и не могат да спрат добре мотивиран атакуващ с нужното ноу-хау. Такъв атакуващ може евентуално да създаде програмно средство, което заобикаля защитата, и да го мултиплицира сред широк кръг потребители. Поради това сигурността, гарантирана от виртуалните стаи за данни, може да бъде загубена напълно във всеки един момент.

3) **Използване на "Enterprise Digital Rights Management"** (eDRM) или понякога **"Information Rights Management"** (IRM) решения. Тези решения включват криптографска защита на документа, която се проверява при всяко отваряне. Те са подобни по замисъл на виртуалните стаи за данни, но са много по-сигурни, тъй като криптографската защита означава, че заобикалянето им е много по-трудно. Най-успешните решения са внедрени в Microsoft Office и макар че изискват платени компоненти, тяхното внедряване е по силата на средно по големина предприятие.

*
* *

Прегледаните мерки за защита демонстрират, че наличието на достатъчна информация е по-важен фактор от наличните средства при информационната сигурност. Наличието на множество решения с отворен код, както и фактът, че в използвания софтуер има заожени достатъчно много функции за прецизна настройка на мерките за сигурност, е положителен факт за МСП и показва, че методическите указания имат потенциал за повишаване на сигурността на МСП.

Разработването и разпространяването на методически указания за информационната сигурност ще бъдат подпомогнати сериозно, ако съществуват агенции и програми, специално ангажирани с тази дейност. Такива агенции функционират

в САЩ и Обединеното кралство, но за съжаление в България все още предстои, подобни агенции да разгърнат дейност.

Прилагането на подобни мерки и методики е полезно дори за МСП, които все още са по-слабо изложени на риск, тъй като натрупването на ноу-хау и трансформирането на фирмената култура отнема време. С разрастването на предприятието и употребата на облачни услуги ненавременното осъществяване на подобна трансформация може да се превърне в основен фактор за подкопаване на информационната сигурност и да доведе до катастрофални преки загуби.

Използвани източници:

Bad bytes Security Blog. (14 Sep 2011 г.). Свалено от http://bad-bytes.blogspot.bg/2011/09/revisting-recent-oscommerce-mass.html

Constantin, L. (13 Oct 2016 г.). *Thousands of online stores compromised by credit-card theft*. Свалено от PC World: http://www.pcworld.com/article/3131040/security/thousands-of-online-shops-compromised-for-credit-card-theft.html

ISO 22301. (2012). *Business continuity management systems - Requirements*. Свалено от https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-1:v2:en

ISO 22313. (2014). *Societal security — Business continuity management systems — Guidance*. Свалено от https://www.iso.org/obp/ui/#iso:std:iso:22313:ed-1:v1:en

ISO 31000. (2009). *Risk management.* http://www.iso.org/iso/home/standards/iso31000.htm.

Meyer, D. (Feb 2016 г.). *Fortune Magazine*. Свалено от Here comes the Post-Safe Harbour EU Privacy Crackdown: http://fortune.com/2016/02/25/safe-harbor-crackdown/

Radeschütz, S., Niedermann, F., & Bischoff, W. (2010). BIAEditor:matching process and operational data for a business impact analysis. *Proceedings of the 13th International Conference on Extending Database Technology, EDBT '10.*

Salter, C. (1998). Towards A Secure Systems Engineering Methodology. *New security paradigms (NSPW'98)*, (стр. 2-10).

Schwartau, W. (Aug 2001 r.). Network Security It's About Time: An Offer for a Metric. *2001*(8), 11-13.

Tjoa, S., Jakoubi, S., & Quirchmayr, G. (2008). Enhancing Business Impact Analysis and Risk Assessment Applying a Risk-Aware Business Process Modeling and Simulation Methodology. *Third International Conference on Availability, Reliability and Security. ARES 08.*

USCERT. (16 03 2017 r.). *Traffic Light Protocol Matrix and Frequently Asked Questions*. Изтеглено на 16 03 2017 г. от https://www.us-cert.gov/tlp

Wrenn, G. (2011). *Ten steps to a successful business impact analysis.* Свалено от TechTarget: http://searchsecurity.techtarget.com/tip/Ten-steps-to-a-successful-business-impact-analysis

Божиков, А. (2014). Облачните услуги и възстановяване от ИТ бедствия и аварии. *Международна научна конференция „Информационните технологии в бизнеса и образованието", ИУ-Варна.*

БИЗНЕС управление

Стопанска академия
„Д. А. Ценов“ – Свищов

Година XXVII, кн. 2, 2017

СЪДЪРЖАНИЕ

МАРКЕТИНГ

ВЛИЯНИЕТО НА ТЪРГОВСКАТА МАРКА ЗА ПОСТИГАНЕ НА КОНКУРЕНТНО ПРЕДИМСТВО – АНАЛИТИЧНО ПРОУЧВАНЕ НА КОМПАНИЯТА ЗА МОБИЛНИ КЛЕТЪЧНИ ТЕЛЕФОНИ „ЗАИН ИРАК“ В АЛ – ДИВАНИЯ, ИРАК
Заки Мухамад Аббас Бхая
Басим Аббас Краиди Ясми 5

ФИРМЕНА конкурентоспособност

ПРОБЛЕМИ И РИСКОВЕ НА КОМЕРСИАЛИЗАЦИЯТА НА ИНОВАЦИИТЕ В РУСКАТА ИКОНОМИКА
Проф. д-р Наталия Голованова
Анна Бекаева 31

ИНФОРМАЦИОННИ И КОМУНИКАЦИОННИ технологии

МЕТОДИ И СРЕДСТВА ЗА ПОВИШАВАНЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ НА ОБЛАЧНИТЕ ИЗЧИСЛЕНИЯ В ПРАКТИКАТА НА МАЛКИТЕ И СРЕДНИТЕ ПРЕДПРИЯТИЯ
Ас. Ангелин Лалев 42

БИЗНЕС практка

АНАЛИЗ НА ФИНАНСОВИТЕ ПОКАЗАТЕЛИ НА ОБЩИНИТЕ В БЪЛГАРИЯ ЗА ЦЕЛИТЕ НА ФИНАНСОВОТО ИМ ОЗДРАВЯВАНЕ
Ас. д-р Дияна Иванова
Ас. д-р Галя Кушева 59

СЪВРЕМЕНЕН ПОГЛЕД ВЪРХУ ПРИЛОЖЕНИЕТО НА СЪВМЕСТНОТО ПОТРЕБЛЕНИЕ В ТУРИЗМА
Доц. д-р Петя Иванова 80

Дадено за печат на 13.06.2017 г., излязло от печат на 22.06.2017 г., формат 70x100/16, тираж 50

ISSN 0861 - 6604

БИЗНЕС управление

ИЗДАНИЕ НА
СТОПАНСКА АКАДЕМИЯ
„Д. А. ЦЕНОВ“ - СВИЩОВ

2/2017

БИЗНЕС управление 2/2017

КЪМ ЧИТАТЕЛИТЕ И АВТОРИТЕ НА СПИСАНИЕ „БИЗНЕС УПРАВЛЕНИЕ“

Списание „БИЗНЕС управление“ **публикува изследователски статии, методологически и методически разработки и прегледи, рецензии, опит.**

1. Обем:
Статии: минимум - 12 страници; максимум – 20 страници;
Прегледи, рецензии, опит: минимум – 5 страници; максимум -10 страници.

2. Депозиране на материалите:
- на хартиен носител и в електронен вид (по E-mail и/или на CD);

3. Технически характеристики:
- изпълнение Word 2003 (минимум);
- размер на страницата - A4, 29-31 реда и 60-65 знака на ред;
- разстояние между редовете 1,5 lines (At least 22 pt);
- шрифт - Times New Roman 14 pt;
- полета - Top - 2.54 см.; Bottom - 2.54 см; Left - 3.17 см; Right - 3.17 см;
- номерация на страницата - долу вдясно;
- текст под линия - размер 10 pt;
- графики и фигури - Word 2003 или Power Point.

4. Оформление:
- наименование на статията, име на автора, научна степен, научно звание - шрифт Times New Roman, 14 pt, с големи букви Bold - центрирано;
- наименование и адрес на месторабoтата; телефони за контакти и E-mail;
- резюме на български език в обем до 30 реда; ключови думи - от 3 до 5;
- **JEL** класификация на публикациите с икономически характер (http://ideas.repec.org/j/index.html);
- основен текст (изложение);
- таблиците, графиките и фигурите се вграждат софтуерно в текста (да позволяват езикова корекция и превод на английски). Цифрите и текстът вътре в тях се изписват с шрифт Times New Roman 12 pt;
- формулите се създават с Equation Editor;

5. Правила за цитиране под линия:
При цитиране да се спазват изискванията на **APA Style (American Psychological Association)**, поместени тук: https://www.uni-svishtov.bg/?page=page&id=71

Всеки автор носи отговорност за отстояваните идеи, съдържанието и техническото оформление на своя текст.

6. Контакти:
Главен редактор: тел.: (++359) 631-66-397
Зам.-главен редактор: тел.: (++359) 631-66-299
Стилов редактор: тел.: (++359) 631-66-335
E-mail: zh.tananeeva@uni-svishtov.bg ; bm@uni-svishtov.bg
Адрес: Стопанска академия „Д .А. Ценов“, ул. „Ем. Чакъров“ №2, Свищов, България