

УПРАВЛЕНИЕ НА МОБИЛНИТЕ УСТРОЙСТВА КАТО КОМПОНЕНТ НА КОРПОРАТИВНАТА ИНФОРМАЦИОННА ИНФРАСТРУКТУРА

Ас. д-р Искрен Любомилов Таиров

Резюме: В условията на цифрова икономика и повсеместно използване на Интернет успешното функциониране на корпоративната ИТ инфраструктура е немислимо без внедряването на техники, технологии и процедури за контрол на достъпа до ресурсите. Поради непрекъснатото популяризиране на мобилни устройства и превръщането им в неразделна част от ежедневието те стават предпочитан способ за достъп до ресурсите на корпоративната информационна инфраструктура. Това налага разработване и реализиране на ефективни решения за управление, базирани на задълбочени анализи и съобразени със спецификата на мобилните устройства.

В настоящото изследване подробно се описва корпоративната ИТ инфраструктура, мобилните устройства като компонент от нея, изследва се използването им и се представят подходящи инструменти за контрол.

Ключови думи: корпоративна ИТ инфраструктура, мобилни устройства, управление.

JEL: L63, L86, M21.

Корпоративната ИТ инфраструктура претърпя сериозно развитие през последните години. Непрекъснато се увеличава броят на преносимите компютри, все по-активно се използва безжична свързаност, също така нараства и броят на лични мобилни устройства, свързани към корпоративната мрежа.

УПРАВЛЕНИЕ НА МОБИЛНИТЕ УСТРОЙСТВА КАТО КОМПОНЕНТ...

Понастоящем мобилните устройства имат впечатляваща изчислителна мощ, произвеждат се големи в количества и тяхната популярност нараства значително по-бързо във всички категории потребители, което води до увеличаване на важността им. Предимно те се използват за забавление, но напоследък се очертава ключовата им роля в постигането на бизнес целите на компаниите за подобряване качеството на живот, а също и за рутинните задачи на хората. По данни на Националния статистически институт (НСИ, 2018), през 2018 г. над 55% от хората в България между 16 и 76 години са използвали мобилен телефон или смартфон за достъп до Интернет извън дома или от работното място. За сравнение прогнозата в световен мащаб е, че над 67% или 4.68 млрд. от населението на земята ще притежава и използва мобилен телефон или смартфон до края на 2019 г. (Statista, 2019).

Много анализатори и специалисти от практиката споделят сходно мнение (CIO, 2011), изразяващо се в това, че масовото използване на мобилни устройства в бизнес средата поставя нови задачи във връзка с мениджмънта на корпоративната ИТ инфраструктура.

Основната **цел** на настоящата статия е да се опише структурата на корпоративната информационна инфраструктура и се постави фокус върху необходимостта от контрол на мобилните устройства като съществен нейн компонент.

Така зададената цел се постига с решаване на следните **задачи**:

- да се определи съставът на корпоративната ИТ инфраструктура;
- да се постави фокус върху мобилните устройства;
- да се изследва използването на мобилни устройства;
- да се представят техники на ефективен контрол.

1. Същност и състав на корпоративната ИТ инфраструктура

Корпоративната информационна инфраструктура (КИИ) се използва за означаване на съвкупността от всички физически устройства и съответния системен софтуер, които изграждат компютърната

мрежа и осигуряват изпълнението на предлаганите от нея общосистемни (мрежови) услуги. Тя се разглежда още като техническа основа за цялата система за управление на вътрешно-фирмената информация. КИИ представлява комплекс от съоръжения, които осигуряват действията на мениджмънта във фирмата. В този смисъл тя е тясно свързана с производителността на управленския труд и неговата ефективност.

Съществуват много научни разработки по темата за ИТ инфраструктура и в частност за състава и компонентите на фирмената ИТ инфраструктура, повечето от които са изградени на базата на предложенията от МакКей и Брокуай **модел** (McKay, 1989), показан на Фигура 1.



Фигура 1. Елементи на ИТ инфраструктура

Според този модел КИИ се определя като съществен елемент за всяка организация, тъй като на основата на КИИ се предоставя възможност за споделяне на информационните технологии. Елементите на КИИ са представени в три слоя:

- най-долният слой (първият слой) е „ит компоненти“. Те включват компютри, принтери, рутери, системи за управление на бази от данни и операционни системи;
- средният слой (вторият слой) е най-просто казано свързан със знанията, уменията, опита, стандартите, необходими за свързва-

УПРАВЛЕНИЕ НА МОБИЛНИТЕ УСТРОЙСТВА КАТО КОМПОНЕНТ...

нето на ИТ компонентите до такава степен, че да могат да се предоставят ИТ услугите, посочени в трети слой;

- най-горният – третият слой се нарича „Споделени ИТ услуги“. В него се включват услуги, които не подлежат на промяна с течение на времето, например управлението на клиентската база данни.

През годините към този модел са добавяни нови елементи от други автори, които са се опитвали също така да определят и опишат ИТ инфраструктурата.

Нашето предложение за осъвременяване на модела на КИИ се свежда до разширяването му със следните компоненти – облачна инфраструктура, мобилни устройства и нови концепции за работа с тях, като BYOx (Bring Your Own Anything – донеси каквото искаш) (Trent, 2013).

Можем да обобщим, че развитието на КИИ е преминало през редица етапи и изследвания, като тези процеси продължават и към настоящия момент. Като извод от представеното дотук, можем да заключим, че становищата на различните автори относно състава и компонентите на КИИ са близки, а самият състав единствено се обогатява през годините спрямо новите технологични достижения. Синтезирано, като състав и компоненти на КИИ бихме могли да посочим следните елементи:

- Компютри и информационна техника;
- Комуникационни мрежи и технологии;
- Компютърни мрежи;
- Софтуер;
 - Операционни системи;
 - Приложен софтуер с общо предназначение;
 - Бизнес софтуер;
- ИТ специалисти;
- Уеб технологии;
- Виртуални и облачни решения и технологии.

В настоящото изследване ще насочим вниманието си към контрола на мобилните устройства и приложения.

2. Изследване използването на мобилни устройства

Мобилните устройства, актуалният подход за ползване на ИТ услуги и възгледът за употреба на персоналните устройства в работата – Bring Your Own Device (BYOD) (IBM, 2017) са един фрагмент от факторите, които оказват съществено влияние върху корпоративната система за контрол. Потенциалната липса на данни или компрометирането им създава множество предизвикателства за ИТ ръководството и специалистите. На база изложеното можем да изведем следните особености при използването на мобилни устройства:

- **Личните устройства добиват още по-широка популярност**

Традиционно, в концепцията BYOD най-общо се схваща, че личните устройства, намиращи приложение за бизнес цели, са смартфони и таблети. Анализаторите отчитат значителна промяна в тази насока – немалка част използваните в работата преносими компютри са собственост на сътрудниците. Според експертите от Forrester (Growder, 2019) ИТ отделите стават все по-гъвкави и проявяват все повече толерантност към BYOD културата, а заедно с това все повече собствени лаптопи намират приложение в работата на служителите. Личните устройства се превръщат в стандартна практика и организацията е необходимо да предприемат необходимите дейности във връзка с това. Според анализаторите все по-мощното търсене на мобилен достъп до компаниите ще доведе до редица важни последиствия, които включват:

- инвестиране в разширяването на отдалечения достъп до съдържание и данни, които обикновено се намират зад корпоративната защитна стена;
- преразглеждане архитектурата на приложенията на компанията и задействане на възможно повече Софтуер като услуга (Software as a Service – SaaS) и платформено независими решения;
- съкращаване на разходите за фиксирани комуникационни услуги и насочване на освободените средства към безжично оборудване и услуги.

Според нас това ще доведе до засилване на проблема с осъществяването на контрол върху тези устройства, което може да увеличи сериозно заплахите относно сигурността на корпоративните данни.

- **Мобилната виртуализация при поискване се превръща във водеща насока при управление на мобилни устройства** (Jaramillo, 2014)

С цел да се изпълнява точно корпоративната политика по отношение на личните устройства, редица организации, които подкрепят BYOD, прилагат технологии за администриране на мобилни устройства, което нерядко се възприема като утежнен и суров подход. Поради тази причина се разработват алтернативни методи за отделяне на лични от корпоративни данни върху личните устройства, като мобилните Virtualized Desktop Infrastructure (VDI), контейнери, обвивки за приложения и инструменти за виртуализация на устройства. Прилагането на тези методи обаче в много случаи въздейства негативно върху потребителския опит и създава рискови предпоставки за КИИ и вчистност за данните. Въпреки направеното, положителният ефект от мобилната виртуализация се очаква да се прояви в недалечно бъдеще. Нашите очаквания са за разработване на технологии, които могат да осигурят възможност за обогатяване управлението на политиките върху целия работен поток от приложения, което ще позволи минимизиране на рисковете за корпорациите.

Според нас тези технологии ще позволят, потребителският опит да остане незасегнат и ще способстват за мобилизацията на корпоративните ресурси. В идеалния случай новите технологии от представеното направление ще могат да се справят изцяло с всички проблеми, свързани с BYOD.

- **Корпоративните приложения на база HTML5 увеличават своята популярност** (Schrock, 2014)

Според множество специалисти приложенията, базирани на HTML5, навлизат в корпоративния сектор с по-висок темп в сравнение с приложения, създадени със специален език за програмиране, като Objective C за iOS и Java за Android. Твърдението се базира на стремежа на американската федерална комисия по комуникациите към разширяване на безжичния спектър от честоти и преследването на по-

ниски разходи за свързаност и по-висока надеждност. По този начин се спомага за разпространението на HTML5, чиито приложения притежават редица предимства, като най-важните от тях са, че те са по-прости и по-евтини за разработка и поддръжка. Това може да доведе до бързо ориентиране на корпоративните приложения в облачната инфраструктура и в недалечно бъдеще организациите ще повишат разходите и за облачни приложения и инфраструктури. По този начин браузърът ще се превърне в основен механизъм за управление на устройствата и е възможно разработването на технологии, които да обезопасят ползването на браузър от мобилно устройство.

- **Мобилните услуги, ориентирани към личността, изискват повишено внимание към поверителността на информацията**

Използването на мобилни устройства предизвиква формирането на нови потенциално резултативни бизнес модели, основани на потребителските предпочитания и действията им в исторически план. Самите устройства са разработени по начин, който осигурява възможност да бъде обединена информация за конкретната личност и нейното електронно присъствие и това може да доведе до сериозни последици. Както е известно, много потребители и организации от дълго време изразяват тревога поради липсата на неясно формирани механизми, регулиращи използването на потребителски мобилни данни. Поради това масовото натрупване на мобилни данни безспорно ще се сблъска със сериозна съпротива. Според множество експерти вероятността за въвеждане на по-строго законодателство за взаимодействието с потребителски данни в мобилната екосистема от регулационните органи е значително малка. Според нас на този фон потребителите ще стават все по-предпазливи относно поверителността на мобилните данни.

3. Инструменти и подходи за управление на мобилни устройства

За успешно управление и контрол на мобилните устройства се препоръчва, те да бъдат включени в обсега на приетите стандарти за

УПРАВЛЕНИЕ НА МОБИЛНИТЕ УСТРОЙСТВА КАТО КОМПОНЕНТ...

управление на достъпа. В допълнение, организациите трябва да поставят фокуса на програмите си за осведомяване по въпросите на управлението на мобилни устройства и по проблемите, отнасящи се до концепцията BYOx (Bring Your Own Anything – донеси каквото искаш).

Като ефективен способ за контролиране на мобилни устройства можем да посочим управлението на корпоративната мобилност (Enterprise mobility management – EMM) (Lirex). Това представлява комплекс от технологии, процеси и политики, насочени към централизиран контрол на използването на мобилни устройства, притежавани от организацията и служителите ѝ.

Чрез технологиите на EMM устройствата и приложенията за корпоративно имплементиране, ползване и актуализиране могат да бъдат конфигурирани, а също осигуряват механизми за подмяна или премахване на достъпа на устройствата до организацията. EMM инструментите се разработват на база концепцията Bring Your Own Device (BYOD), според която множество компании не ограничават мобилните устройства на работното място, а се прилагат EMM решения, с помощта на които се осъществява гъвкавост на потребителите, а в същото време се запазва и пълен ИТ контрол.

Чрез EMM технологиите може да се извърши проследяване и инвентаризиране на устройствата, настройките и ползването им, също и установяване съответствието на корпоративните политики и управление на средствата за достъп.

Основно EMM решенията се осъществяват чрез:

- добавяне на контрол за шифриране на данните;
- права за достъп до данни;
- споделени устройства;
- приложение за опаковане и контейнери;
- "заключване" на устройството.

Чрез изброените способности ИТ отделът ще бъде в състояние да констатира и проследява проблемни ситуации, свързани с достъп на мобилни устройства до мрежата чрез инвентаризация, анализ и отдалечено управление.

Съществуват разработени EMM решения на VM ware, Symantec, Checkpoint, Microsoft, Sophos.

Практиката показва обаче, че прилагането само на EMM не е достатъчно. В допълнение на EMM е необходимо и управление на мобилните приложения.

Управлението на мобилни приложения – Mobile application management (MAM) (Mobile Application Management) се отнася до софтуера и услугите, които осигуряват и контролират достъпа както за смартфони и таблети, притежавани от служители, така и за компании, за мобилни приложения в бизнес контекст. Въпросните мобилни приложения могат да бъдат или комерсиално достъпни за обществеността, или да бъдат разработени вътрешно в компанията. Управлението на мобилни приложения се различава от управлението на мобилно съдържание (Mobile content management – MCM) (Contentful) и управлението на мобилните устройства (Mobile device management – MDM) (Itforce, 2013), тъй като се фокусира върху приложения, които устройствата използват, а не върху управлението на самите устройства или на съдържанието в тях. MAM позволява на системния администратор да има по-малко контрол над устройствата, но по-голям контрол върху техните приложения, докато MDM може да включва и двата вида управление.

С MAM системата компанията може да контролира какви мобилни приложения предоставя на служителите си, когато тези приложения се актуализират и когато се премахват от устройствата. Като цяло MAM включва магазин за приложения на предприятия, който е подобен на типичния магазин за приложения на мобилно устройство за целите на предоставянето на актуализации и добавянето и премахването на приложения от употреба. Това също така позволява на компанията да следи как работи приложението и как се използва. В допълнение системният администратор ще може дистанционно да премахва или изтрива всички данни от тези приложения.

Основните характеристики на системата MAM включват доставка, актуализиране, опаковане, управление на версиите и конфигурациите, мониторинг на производителността, проследяване и отчитане, управление на събития, анализ на употребата, удостоверяване на потребителя, push услуги, отчитане на сризове и удостоверяване на потребителя. Тъй като мобилните устройства стават много по-широко използвани в света на бизнеса, възможността да се използват тези функции в редица устройства и операционни системи, се превръща в много по-належащ проблем, който може да бъде решен със системата MAM.

УПРАВЛЕНИЕ НА МОБИЛНИТЕ УСТРОЙСТВА КАТО КОМПОНЕНТ...

Във връзка със системите за управление на мобилни устройства експертите от Forrester Research публикуват доклад с 10 основни пункта (CIO, 2011):

- за различните сътрудници ИТ отделът трябва да осигури различни нива на поддръжка на мобилни технологии;
- за да разберат потребностите и предпочитанията на сътрудниците, ИТ специалистите трябва да зададат подходящите въпроси;
- препоръчително е да се разработи единна и ясна политика за прилагане на корпоративните и личните мобилни устройства;
- необходимо е запознаване с ограниченията на мобилните платформи и съответно осигуряване на приоритетна поддръжка за платформите, които най-много се нуждаят от такава;
- MDM решенията не са подходящи за всяка платформа;
- препоръчително е да се създават стимули за ИТ доставчиците да откриват електронни магазини, които биха били полезни за компанията;
- използване на виртуализация за предоставяне на достъп до приложения на Windows потребители, които нямат тази операционна система върху своето устройство;
- поддържане личните устройства на служителите, слагане на строги ограничения за тяхното използване;
- уведомяване на потребителите какви мобилни услуги са одобрени;
- обмисляне на евентуална компенсация на цената на обслужването.

Като механизми за осъществяване на превенция срещу рисковете, свързани с мобилни устройства, можем също да посочим някои правила, които мениджмънтът да насочи към собствениците на устройствата:

- сваляне на приложения само от официални източници;
- избягване отваряне на подозрителни линкове;
- избягване обществените Wi-Fi мрежи и задължително включване на VPN към устройството;
- избягване използването на най-важните приложения, напр. тези за мобилно банкиране, извън средата на защитената домашна или офис мрежа;

- да не се поставят отметки на опциите “неизвестни източници” и “режим на разработчик” в настройките на мобилното устройство;
- определяне на допустимите видове устройства (само предоставени от предприятието срещу разрешението за употреба на лични устройства и такива, като например BlackBerry или iPhone);
- определяне характера на услугите, достъпни чрез устройствата, като се вземе предвид съществуващата ИТ архитектура;
- определяне на начина, по който служителите използват устройствата, отчитайки корпоративната култура, човешките фактори;
- интегриране на всички издадени от предприятието устройства в едно приложение за управление на информационните активи;
- описание на вида на автентичността и криптирането, присъщи на устройствата;
- очертаване на задачите, за които служителите могат да използват устройствата и видовете приложения, които са позволени;
- изясняване как данните трябва да бъдат сигурно съхранявани и предавани.

Можем да обобщим, че мобилните устройства са сред основните предизвикателства за осъществяване на ефективен контрол и управление през последните години. Организациите се опитват да се преборят с проблемите с мобилни компютърни устройства, собственост на работодателя или служителя.

Решаването на тези проблеми е неразривно свързано със създаването на правила и култура на поведение, които задължително да се спазват в рамките на организацията. За осъществяването на тези дейности се изисква време и усилия не само от технологичен, но и от социален характер. Важно е да се разработи и предложи превантивна политика, която да отчита потенциалните проблеми, а обществото следва постоянно да бъде информирано за появата на нови такива, които непрекъснато ще се появяват заедно с технологичните усъвършенствания. Ефективното преодоляване на проблемите с мобилните устройства ще осигури сериозни конкурентни предимства на организацията, също и високо ниво на удобство, удовлетвореност и сигурност на служителите.

УПРАВЛЕНИЕ НА МОБИЛНИТЕ УСТРОЙСТВА КАТО КОМПОНЕНТ...

* * *

Мениджмънтът на мобилните устройства се е развил до такава степен, че дори строго регулираните индустрии са се насочили към позволяване на служителите си да използват одобрени от компанията устройства за комуникации и бизнес дейности, както и развлечения като достъп до социални медии и мрежи, игри и други. Ползите при използването и управлението на мобилни устройства и приложения, заедно с бързите темпове на „мобилизиране на служителите“ и очакваното въздействие върху способността на организацията да подсигурава корпоративни данни, разположени върху една все по-разнообразна колекция от мобилни устройства, собственост на служителите, насочва мениджмънта към засилен интерес за допълнения или алтернативи на концепцията BYOD. Като такива могат да бъдат управлението на мобилни приложения (Mobile application management – MAM), управлението на корпоративната мобилност (Enterprise mobility management – EMM) и вътрешни правила за контрол.

Използвани източници

CIO. (15 12 2011 г.). Управление на мобилните устройства – 10 урока от Forrester. Изтеглено на 20 03 2019 г. от CIO.bg: http://cio.bg/4299_upravlenie_na_mobilnite_ustrojstva__10_uroka_ot_forrester/

Contentful. (н.д.). Mobile CMS: a comprehensive overview. Изтеглено на 21 02 2019 г. от <https://www.contentful.com/r/knowledgebase/mobile-cms/>

Growder, J. H. (18 01 2019 г.). The Future Of Enterprise Computing. Изтеглено на 18 03 2019 г. от <https://www.forrester.com/report/The+Future+Of+Enterprise+Computing/-/E-RES142617>

- IBM. (2017). Bring your own device. Изтеглено на 19 03 2019 г. от <https://www.ibm.com/security/mobile/maas360/bring-your-own-device>
- Itforce. (4 09 2013 г.). MOBILE DEVICE MANAGEMENT - AN OVERVIEW. Изтеглено на 16 03 2019 г. от <https://www.itforce.ie/blog/mobile-device-management-an-overview>
- Jaramillo, D. F. (2014). *Virtualization Techniques for Mobile Systems*. Springer.
- Lirex. (н.д.). EMM. Изтеглено на 06 03 2019 г. от <http://lirex.bg/home/основни-направления-на-лирекс/киберсигурност/защита-на-устройства/mdm/>
- McKay, D. B. (1989). *Building IT infrastructure if the 1990s Stage by stage*. Nolan Norton & Company.
- Mobile Application Management. (н.д.). Изтеглено на 16 02 2019 г. от <https://www.kony.com/resources/glossary/mobile-application-management/>
- Schrock, A. (28 08 2014 г.). HTML5 and openness in mobile platforms. *Continium*, 28, стр. Pages 820-834.
- Statista. (2019). *Number of mobile phone users worldwide from 2015 to 2020 (in billions)*. Изтеглено на 21 06 2019 г. от [statusta.com: https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/](https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/)
- Trent, R. (11 06 2013 г.). BYOx: Bring Your Own Anything Announced at TechEd 2013. Изтеглено на 15 03 2019 г. от <https://www.itprotoday.com/compute-engines/byox-bring-your-own-anything-announced-teched-2013>.
- НСИ. (17 12 2018 г.). *Използване на мобилни устройства от лицата за достъп до интернет*. Изтеглено на 21 06 2019 г. от Национален Статистически Институт: <http://www.nsi.bg/bg/content/2820/използване-на-мобилни-устройства-от-лицата-за-достъп-до-интернет>

БИЗНЕС управление

Стопанска академия
„Д. А. Ценов“ – Свищов

Година XXIX, кн. 3, 2019

СЪДЪРЖАНИЕ

МЕНИДЖМЪНТ практика

ИНДИКАТИВНИ МОДЕЛИ ЗА РАЗВИТИЕ НА МЕДИТЕ В ГЛОБАЛНАТА ИКОНОМИКА

Андрей Чужиков 5

СЪСТОЯНИЕ И НАСОКИ ЗА РАЗВИТИЕ НА АДМИНИСТРАТИВНОТО ОБСЛУЖВАНЕ В ОБЩИНИТЕ

Доц. д-р Катя Емилова Кирилова 25

ИЗСЛЕДВАНЕ НА СИТУАЦИОННОТО ПОВЕДЕНИЕ НА ЧОВЕШКИЯТ ФАКТОР В ОРГАНИЗАЦИЯТА

Снежина Иванова 46

ИНФОРМАЦОННИ И КОМУНИКАЦИОННИ технологии

УПРАВЛЕНИЕ НА МОБИЛНИТЕ УСТРОЙСТВА КАТО КОМПОНЕНТ НА КОРПОРАТИВНАТА ИНФОРМАЦИОННА ИНФРАСТРУКТУРА

Ас. д-р Искрен Любомилев Таиров 64

ГЪВКАВА МЕТОДОЛОГИЯ ЗА УПРАВЛЕНИЕ НА БИЗНЕС ПРОЦЕСИ В ИТ КОМПАНИЯ

Ас. д-р Станимира Йорданова
Докторант Климент Тошков 77

Редколегия на сп. „Бизнес управление“

Красимир Шишманов – главен редактор, Стопанска академия „Д. А. Ценов“ - Свищов

Никола Янков – зам. главен редактор, Стопанска академия „Д. А. Ценов“ - Свищов

Иван Марчевски, Стопанска академия „Д. А. Ценов“ - Свищов

Ирена Емилова, Стопанска академия „Д. А. Ценов“ - Свищов

Любчо Варамезов, Стопанска академия „Д. А. Ценов“ - Свищов

Румен Ерусалимов, Стопанска академия „Д. А. Ценов“ - Свищов

Силвия Костова, Стопанска академия „Д. А. Ценов“ - Свищов

Международна редколегия на сп. „Бизнес управление“

Александру Неделеа – Университет „Стефан Велики“, Сучава, Румъния

Дмитрий Владимирович Чистов, – ФГОБУ ВПО Финансов университет при правителството на руската федерация, Москва, Русия

Йоана Панагорец – Университет Валахия, Търговище, Румъния

Йото Йотов – Драксел университет, Филадельфия, САЩ

Махмуд Ел Батран – Университет Кайро, Кайро, Египет

Наталья Борисовна Голованова – Московски технологически университет, Москва, Русия

Татяна Викторовна Орехова – Донецки национален университет, Виница, Украйна

Тадиа Джукич —Университет в Ниш, Ниш, Сърбия

Ян Тадеуш Дуда – АГН Университет за наука и технологии, Краков, Полша

Виктор Чужиков – Киевски национален икономически университет "Вадим Гетман", Киев, Украйна

Стилов редактор – Анка Танева

Превод на английски език – ст. преп. Цветана Шенкова,

ст. преп. Даниела Стоилова, ст. преп. Иванка Борисова

Превод на руски език – ст. преп. Ирина Иванова

Технически секретар – ас. Живка Тананеева

Отпечатването на списанието за 2019 г. се осъществява с безвъзмездната финансова помощ на Фонд "Научни изследвания" - НП 07/58, съгласно Договор КП-06-НП/36 от 12.12.2018, по конкурс "Българска научна периодика - 2018 г."

Дадено за печат на 09.09.2019 г., излязло от печат на 16.09.2019 г.,
формат 70x100/16, тираж 100

© Стопанска академия „Димитър А. Ценов“ – Свищов,
ул. „Ем. Чакаров“ 2, тел.: +359 631 66298

© Академично издателство „Ценов“, Свищов, ул. „Градево“ 24

ISSN 0861 - 6604

БИЗНЕС управление

БИЗНЕС управление 3/2019

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



3/2019

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. Депозирание 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 местоработата; 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