

ОТНОСНО ЗНАЧЕНИЕТО НА ВЪТРЕШНИЯ КОНТРОЛ ЗА БАНКОВАТА СИГУРНОСТ

Светла Михайлова Боянова
Стопанска академия „Д. А. Ценов“ – Свищов
Катедра „Финанси и кредит“
e-mail: sboyanova@agrion.bg

Резюме: Въпреки утвърдените и прилагани практики и модели за контрол върху банковата дейност, наблюденията в публичното пространство през последните години показват, че зачестяват различните форми на злоупотреби от страна на банкови институции спрямо депозитори и клиенти на институциите. Същевременно нараства броят на рисковите банкови експозиции, което е индикатор за съществуването на пропуски, респ. слабости в системата за контрол. Във връзка с това в статията се очертават някои проблеми с документалната безопасност на банковата информация и по-конкретно документни измами от трети лица, документни измами от вътрешни за банката лица, загуба, кражба или злоупотреба с банкова и фирмена информация, конфликт на интереси, скиминг измами, участие и прикриване на финансови престъпления и т.н.

Ключови думи: Вътрешен контрол, одит, риск, хакерска атака, лични данни.
JEL: 21.

ON THE IMPORTANCE OF INTERNAL BANK SECURITY CONTROL

Svetla Mihaylova Boyanova
D. A. Tsenov Academy of Economics – Svishtov
Department of Finance and Credit
e-mail: sboyanova@agrion.bg

Abstract: Despite the established and applied banking control practices and models, the observations in public space in the past years have shown an increase in the number of the various forms of abuse by banking institutions against depositors and clients. At the same time, the number of risky bank exposures has been going up, which is an indicator of the existence of gaps, respectively weaknesses in the control system. In this regard, the article outlines some problems with the documentary security of banking information and in particular document fraud by third parties, document fraud by bank insiders, loss, theft or misuse of banking and corporate information, conflict of interest, skimming fraud, involvement and concealment of financial crimes, etc.

Keywords: Internal control, audit, risk, hacking attack, personal data.
JEL: 21.

Въведение

За да се гарантира надеждна защита на икономическите агенти, банковата система задължително подлежи на контрол. В основата на конт-

ролната дейност на всяка банка стои анализът на текущото ѝ състояние, идентифициране на проблемните, критичните точки при предварително зададени прогнозни параметри, определяне на методите, способите и формите на контролно въздействие и оценка на нормата на поведение на системата, респ. единицата, при предварително зададените ограничителни условия. Това определя актуалността на разглежданата проблематика.

Обект на настоящата статия е вътрешнобанковият контрол, а *предметът* на изследването е фокусиран върху проблемите на вътрешния контрол в кредитните институции. Основната *цел* на разработката е да се очертаят някои възможности за усъвършенстване на вътрешния контрол в банките. Постигането на тази цел изисква решаването на следните *важни задачи*: 1) открояване на особеностите на вътрешния контрол в банките; 2) разглеждането на някои съществуващи проблеми с документалната безопасност на банковата информация.

Основните прийоми, използвани в изследването, са методите на анализ и синтез, както и методите на индукция и дедукция.

1. Особенности на вътрешния контрол в банките

Системата за вътрешен контрол се характеризира със своите обекти и субекти. Обектите на този контрол са дейности, операции, институционални обекти, т.е. това, което се проверява. Субектите на контролната дейност са инспекторите, одиторите, ревизорите, финансовите контролори и други, които го осъществяват.

Контролният процес в банковите институции трябва да бъде постоянен, за да може успешно да бъде проследявано, дали се постигат предварително поставените цели и задачи; адекватно и оперативно ли се контролират различните рискове, отнасящи се до банковата дейност; налице ли е надеждност и цялостност на финансовата и управленска информация; съществува ли целсъобразност и законосъобразност на дейностите по банкирането и др.¹

Банковият контрол е всеобхватен, т.е. налице е вътрешен и външен контрол. Във връзка с това се различават: предварителен надзор (осъществяван още при учредяване на търговските банки чрез издаване на лицензия или други разрешения – напр. ликвидация), текущ контрол – (извършван по време на реализирането на банковата дейност чрез отчетите, които търговските банки представят в БНБ) и последващ контрол (контролът върху дейността на търговските банки).

Надзорът обхваща най-общо идентифициране на състоянието на капитала на банката, кредитната дейност, спазването на лицензията.

¹ *Заб.*: това е заложено в чл. 2, ал. 1 от Наредба №10 за вътрешния контрол в банките, обн. ДВ, бр.102 / 2006.

Според нормативната уредба² основна цел на банковия контрол е поддържането на стабилността на банковата система и сигурността на вложителите. Като функция на управлението банковият контрол може да се представи като неразделна част от процеса на функциониране на всяка банка. Характерна негова особеност е съвместяването на контролните функции с банковите операции (Динев, 1999). В този смисъл той е съставен елемент от технологичните операции във всяка банка, доколкото протича успоредно с банковите операции.

Томов (2009) посочва, че банковият контрол е свързан с безналичните плащания, с кредитните и депозитните операции. В неговия обхват се включват и валутните операции, преводите и операциите с ценни книжа. В неговия труд банковият контрол е представен, че се извършва от вътрешнобанкова структура (т.нар. вътрешен контрол) и такъв, осъществяван от външна за банката структура (известен като външен контрол, извършван от централната банка или надзорен съвет, от специализирани одиторски предприятия или структури за финансово разузнаване).

Основните елементи на вътрешния контрол са управленският контрол, контролът на риска, отчетността и информацията и вътрешният одит.³ Управленският контрол според законодателя се свежда до:

- ✓ преглеждане на организационната структура на банката и евентуални организационни и структурни трансформации;
- ✓ създаване на ред за определяне и делегиране на правомощията и отговорностите на администраторите;
- ✓ изграждане на стратегия и план за дейността на банката и проследяване на тяхната реализируемост;
- ✓ политика за управление и контрол на риска;
- ✓ ред за изготвяне и обхват на управленската информация;
- ✓ организация на оперативния контрол, вкл. правилата и процедурите по одобряване, изпълнение и отчитане на операциите, осъществявани в банката;
- ✓ вътрешни правила и процедури за наблюдение на риска и ефективността на контролните системи, докладване на установените слабости в дейността на организацията и структурните ѝ звена;
- ✓ проследяване на спазването на Кодекса за етично поведение на администраторите и служителите;
- ✓ система за обучение, оценка и стимулиране на лицата, заети с контролни и изпълнителни функции в банковия сектор.

² *Заб.*: тук се има предвид преди всичко постановките, заложи в чл. 2, ал. 6 от ЗБНБ и чл. 4, ал. 1 и чл. 79 – 103 от Закона за кредитните институции, и няколко подзаконови нормативни акта на БНБ, в частност Наредбата за капиталовата адекватност.

³ *Заб.*: Съгласно чл. 4 на Наредба №10 за вътрешния контрол в банките, обн. ДВ, бр. 102 / 2006

Контролът на риска се заключава в поддържането на определена система за контрол, включваща:⁴

- определянето на количествено измерими и неизмерими за банката рискове;
- управлението на риска и на моделите за оценка на рисковете;
- периодичен преглед на рисковата матрица на банката;
- наблюдение и периодична оценка за съответствие на вътрешните правила за управление на риска в банката, съобразно пазарните условия и добрата банкова практика;
- вид, структура и периодичност на отчетите за риска и др.

Относно отчетността и информацията всяка банка е задължена да поддържа своя система за отчетност и информация, която да осигурява бърз достъп до информационните ресурси и тяхното движение за целите на банковата институция и свързаните с нея заинтересовани страни. В законодателната рамка е посочено, че всички финансови сделки и банкови операции се регистрират своевременно и изчерпателно в хронологичен ред. За целта банките поддържат електронни файлове и досиета на сделките по видове операции, клиенти и други избрани от тях критерии и принципи. Изискването към банковите досиета е да съдържат опис на документите в досието, протоколи, споразумения, договори и други; да съдържат информация за клиентите и пазара, както и други документи от съществено значение за банката в качеството ѝ на администратор на лични данни и класифицирана информационна база данни.

Кадрите, осъществяващи съответните банкови дейности и контролни функции, следва да притежават професионални умения за прилагането на стандартите за професионална практика на вътрешен одит, процедурите и техниките за извършване на одит; да имат познания и опит в прилагането на счетоводните стандарти и познания за принципите на управление и добрата банкова практика, както и да защитават интересите не само на акционерите и кредиторите на банката, но и на клиентите. Те следва да спазват разпоредбите на Наредбата за класифицираната информация⁵, регламентираща предотвратяването на нерегламентиран достъп или на опит за такъв до класифицирана информация; предотвратяване, пресичане и установяване на действия, които поставят под съмнение надеждността на служителите и групиране на служителите, съобразно издаденото им разрешение за достъп до класифицирана информация, както и своевременното установяване и противодействие при опит за нарушаване на физическата сигурност на информацията и Закона за защита на личните дан-

⁴ *Заб.*: Съгласно Наредба № 10 от 2006 г.

⁵ *Заб.*: има се предвид чл. 8, ал. 4 и 5 от Наредбата за системата от мерки, способности и средства за физическата сигурност на класифицираната информация и за условията и реда за тяхното използване, ПМС№52 / 2003.

ни⁶. В последния е указано, че личните данни трябва да се обработват законосъобразно и съвместно и да се събират за конкретни и точно определени законни цели, като не се допуска допълнителното им обработване за несъвместими с посочените в клаузите на съответния договор между институцията и клиента, цели. Това прави ограничаването на риска от нарушаване на безопасността на банковата информация основна задача за съвременните банкови институции. За да се ограничи този риск, трябва много внимателно да се анализират различните възможности за нарушаване на тази безопасност, като се има в предвид динамичното развитие на възможностите за накръняването ѝ.

2. Проблеми с документалната безопасност на банковата информация

Проблемите с документалната безопасност на банковата информация най-често са свързани с:

● **Документни измами от трети лица** – документните измами от трети лица обикновено са свързани с използване на фалшифицирани документи (лични карти, фирмени документи, платежни инструменти). Чрез тях се извършва непосредствено присвояване на финансови средства или се създава част от цялостна мрежа за извършване на значително по-големи по размер финансови престъпления. Сравнително чести, но с ограничен финансов ущърб за банката, са измамите, свързани с фалшиви платежни инструменти (валута, чекове, карти, платежни нареждания), при които външно за банката лице, в замяна на тях и най-често еднократно, придобива определено количество пари. Обикновено в този тип измами рядко има замесени вътрешни лица, доколкото самите те биха били обект на финансови и административни санкции за ненавременното установяване на фалшивите документи. Макар и в по-редки случаи поради относително по-високия риск, чрез неистински документи е възможно да бъдат изтеглени банкови кредити, издадени кредитни карти или карти с овърдрафт, фирмени кредитни линии, банкови гаранции, акредитиви и др. В тези случаи е необходима значително по-сериозна подготовка от престъпната група, като много често в нея участва и вътрешно за банката лице. Тук финансовите щети за нея са много по-големи, като в определени случаи, извън преките финансови загуби, тя понася и индиректни щети в резултат на влошена репутация и имидж и загуба на доверие от страна на нейните клиенти и контрагенти. Масова практика е хора, които заминават за дълго в чужбина, да подписват пълномощни. Те дават възможност на трети лица да ги представляват пред конкретна банка. Често се случва и

⁶ *Заб:* по-конкретно става дума за чл.2, ал.2, т.1 и 2 на Закон за защита на личните данни, обн. ДВ, бр.81 / 2016.

трудноподвижни хора да използват тази услуга, а причината е, трети лица да могат да извършват тегления и плащания. Освен че процедурата е изключително ангажираща (нужна е заверка от нотариус и др.), нотариалната заверка на съдържанието на пълномощното не дава гаранция, че пълномощникът няма да злоупотреби с правата, които то му дава. Според проучвания, от 80% от измамите с пълномощни се случват точно във времето, когато те бъдат оттегляни. Има едни 3-4 часа, докато бъде отразено в регистрите на банката и точно в този диапазон злоупотребите са най-много (Bowker, 2012).

● **Документни измами от вътрешни за банката лица** – тези измами са съществен риск за финансовите институции. Сред основните мотиви за извършване на престъпление от персонала са желанието за бързо забогатяване, решаване на неотложни финансови проблеми, хазартен начин на живот, а в определени случаи и натиск от външна страна – партньор или криминален контингент. Те се осъществяват както самостоятелно от отделни банкови служители, мениджъри или собственици, така и със съдействието на подставени лица или криминални групи, като е налице пряка връзка между положението в банковата йерархия и нанесената на институцията щета. Вътрешнобанковите документни измами най-често са свързани с присвояване на средства от чужди сметки, теглене на банкови кредити и издаване на банкови карти на името на трети лица, както и присвояване на средства чрез фалшива фирма по линия на търговското кредитиране, банковите гаранции и авансови плащания. Вътрешно лице е всяко лице, което притежава вътрешна информация. Злоупотреба с вътрешна информация възниква, когато дадено лице разполага с вътрешна информация и я използва, като придобива или се разпорежда за собствена сметка или за сметка на трета страна, пряко или косвено, с финансови инструменти, за които се отнася тази информация. Използването на вътрешна информация посредством отмяна или изменение на нареждане относно финансов инструмент, за който се отнася информацията, когато нареждането е направено, преди съответното лице да разполага с вътрешната информация, също се счита за злоупотреба с вътрешна информация.

Забранено е препоръчването или склоняването на друго лице да участва в злоупотреба с вътрешна информация. Лице може да притежава вътрешна информация в резултат на:

- а) дялово участие в капитала на емитента;
- б) достъп до информацията чрез упражняване на дейност, професия или служебни задължения;
- в) участие в престъпна дейност;
- г) притежаване на вътрешна информация при обстоятелства, различни от посочените, когато лицето знае или е следвало да знае, че това е вътрешна информация;

д) с участието си при вземането на решението да се извърши придобиването, разпореждането или отмяната или изменението на нареждане за сметка на инвестиционния посредник (Bowker, 2012).

● **Загуба, кражба или злоупотреба с банкова и фирмена информация.** Пряко свързан с този аспект на нарушаване на банковата сигурност са и престъпленията, отнасящи се до загуба, кражба или злоупотреба с банкова и фирмена информация. В определени случаи те се извършват пряко или косвено с помощта на банкови служители. Обект на основното финансово престъпление е засегнатата фирма или лице, а участieto и загубите на банката са само част от много по-голяма и цялостна схема, включваща измамни фирми, клиенти и партньори. По този начин е възможно, банката и нейните служители да се окажат участници в извършването и прикриването на финансови престъпления, които могат да включват в себе си и елементи на укриване на данъци, пране на пари и финансиране на криминални и/или терористични организации (Bowker, 2012).

● **Конфликт на интереси** – той е налице, когато между членове на едно семейство (съпруг/съпруга; роднина по права линия (деца); брат, сестра; лице във фактическо съпругеско съжителство; съпруг/съпруга на дете; дете на съпруг/съпруга в случай, че детето е от друг брак; брат, сестра на съпруг/съпруга; съпруг/съпруга на брат, сестра) се създаде отношение на пряко управление или контрол в банката. Отношение на управление е връзка между двама служители, единият от които по силата на служебното си положение е ръководител на другия (например съпруг-съпруга). Отношение на контрол е връзка между двама служители, единият от които заема позиция в структурно звено в Централното управление на банката с контролни функции, а другият – в структурно звено с други функции или в поделение на банката.

Придобиване на конфиденциална информация с цел различни форми на шпионаж, като мотивите най-често са свързани с проучване на бизнес или семеен партньор, както и за придобиване на вътрешна информация и използването ѝ за бъдещо обогатяване. Използване на банковата инфраструктура за финансови и данъчни престъпления. Извън преките финансови, търговски и данъчни измами, в които са замесени банкови сметки на реални и/или фиктивни лица и фирми, организираната престъпност използва банковата система в опитите си за прикриване на истинския произход на придобитите от нелегална дейност парични средства и тяхното легализиране и интегриране в икономиката (процес, познат като „пране на пари“).

● **Скиминг измамните.** С все по-широкото използване на Интернет и мобилните устройства за финансови трансакции нарастват опасностите от измами. Сред най-разпространените в България са злоупотребите с карти, фишингът и заразяването със зловреден код. Чрез скиминг схемите се източват пари от потребителски сметки. Измамниците разчитат на данните, съхранявани в магнитните ленти на банковите карти. Те стигат до тях, като върху карточетящата технология на банкомата инсталират ново уст-

ройство, записващо тази информация. Четирицифреният PIN код се набавя чрез камера, инсталирана в близост до машината, така че да има видимост към клавиатурата. Цялата процедура отнема не повече от 20 секунди. Данните са достатъчни за произвеждането на т.нар. “бели пластики” и извършване на злоупотреби (Bowker, 2012).

● **Участие и прикриване на финансови престъпления.** Все по-широкото навлизане на високотехнологичните иновации в банковите продукти и услуги, позволяващи пълно функционално банкиране от всяка точка на земното кълбо, повишава изкушението за бързо забогатяване. Този тип опити за присвояване отдавна не са запазена територия единствено за хакерите. От тази гледна точка информационната безопасност на банковата дейност се превръща в ключов аспект от цялостната банкова сигурност.

Най-честите направления, в които се правят опити за присвояване, манипулиране или унищожаване на банковата информация, са свързани с реализацията на престъпления или престъпни схеми за:

- измами, засягащи идентичността;
- измами, свързани с шпионаж;
- използване на съществуващата финансова инфраструктура;
- разрушителни атаки.

Най-честите и широко разпространени престъпления, отнасящи се до информационната сигурност, са тези, свързани с присвояване на чужда идентичност. Те се проявяват в две основни направления: 1) кражба на съществуващи сметки и финансови инструменти на трето лице и 2) създаване на сметки и придобиване на финансови инструменти с фалшива самоличност (откраднати или изцяло фалшифицирани документи). Докато целта на престъпленията от първото направление е неправомерно отнемане на чуждо имущество с цел обогатяване, то тези от второто най-често представляват част от значително по-голяма престъпна схема – създаване на фиктивна самоличност с цел осъществяване на търговски, финансови, застрахователни или данъчни измами. Значителният дял на сенчестата и ъндърграунд икономика, както и засилените процеси по финансиране на терористични и радикални групировки, поражда остра нужда от изграждането на ефективни схеми и способности за прикриване на истинския произход на паричните средства. Това, съчетано с навлизането на високите технологии в банковата сфера, процесите на глобализация и създаването на световни офшорни зони, правят изключително примамливо използването на банковата инфраструктура за пране на пари. Много често за целите на този процес се използва значителна част от описаните по-горе прийоми, съчетавайки както пряко участващи или подставени лица, така и кражба на реални сметки и създаване на сметки с фалшива самоличност. През последните десетилетия придобиването на конфиденциална банкова информация трайно се нареди сред арсеналите на икономическия и индустриален шпионаж, като през последните години към подобен способ при-

бягват дори и държави. Престъпленията от първия тип обикновено са движени от мотиви, свързани с проучване на бизнес партньор, придобиване на вътрешна информация с цел борсови спекулации, а в определени случаи и проучване на поведението и финансите на семейния партньор. Въпреки че държавата осъществява контрол върху банковата дейност, достъпът до лична банкова информация обикновено е ограничаван от законите за банковата тайна. Държавата винаги има вратички за придобиване на подобна информация по легален начин, но процедурата е тежка, а разрешените случаи изискват решение на съда след предоставяне на убедителни доказателства за извършени или извършващи се престъпления. Интересно е да се отбележи, че през последните години се наблюдава промяна в този подход, като държавата или сама се намесва в този процес, основно чрез следене на финансовите трансакции за предотвратяване прането на пари, или сключва сделки с трети лица за придобиване на подобна информация за установяване на данъчни престъпления.

През последните години значително се увеличават хакерските атаки към финансовите институции, като нанесените щети се изчисляват на милиарди. Наред с традиционния мотив за бързо обогатяване, много често е налице проява на т.нар. хакерство за забавление. При него целта е не толкова кражбата на пари, колкото доказването на интелектуалното превъзходство и възможността за разбиване на банковата защита.

За съжаление все по-често ставаме свидетели и на т.нар. кибертероризъм, чиято цел е тотално унищожение на информацията, прекъсване на нормалните бизнес процеси, вкл. и в банките, и създаване на хаос в държавата. Прибягването до подобни похвати и прийоми обикновено е свързано с прикриване на следи от престъпления чрез цялостно унищожаване на достъпна текуща и архивна информация. В определени случаи банките могат да се окажат индиректна цел в рамките на съвкупни мероприятия в цялостна информационна война между различни държави.

Тази година една от най-големите български банки – Банка ДСК – бе обект именно на такава атака. В официално съобщение към медиите⁷ на 23 юни 2019 г. ръководството на банката съобщи, че е получила предупреждение от български гражданин, че притежава информация, съдържаща клиентски данни от банката. След направено разследване се установява, че лицето е осъждано и лежало в затвора за банков обир. Ръководството назначава вътрешно разследване, което установява, че няма успешна дигитална атака срещу информационните системи на банката и информира КЗЛД (Комисия за защита на личните данни) за създалата се ситуация. В самото уведомление банката подчертава, че ако въпросното лице наистина притежава такива данни, то те са получени по друг, но също така незаконен начин с неправомерно действие в нейна вреда.

⁷ *Заб.:* <https://dskbank.bg/новини-и-промоции/детайли/2019/08/29/изявление-на-банка-дск-относно-решение-на-кзлд>

Проверката на комисията е проведена в едномесечен срок. Установява се, че при осъществяването на дейността си банката в качеството на администратор на лични данни не е предприела и приложила необходимите технически и организационни мерки, за да осигури и гарантира постоянната поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване на лични данни на физически лица (клиентите) и свързаните с тях трети лица. Именно тези пропуски са довели до осигуряване на възможност за неправомерно разпространяване и достъпване на личните данни на клиентите. Изтекли са данни като трите имена, гражданство, ЕГН, постоянен или настоящ адрес, копия на личните карти и съдържащите се в тях биометрични данни за ръст и цвят на очите; всички лични данни, съдържащи се в данъчни документи, удостоверяващи доходи и здравноосигурителен статус на кредитополучателите и трети лица по тях, както и данни за здравословно състояние (като в някои кредитни досиета се съдържат решения на ТЕЛК за намалена работоспособност), номера на разплащателни сметки, както и регистрационни номера и дати на нотариални актове с положени подписи.

Председателят на КЗЛД Венцислав Караджов, в свое интервю пред БТВ⁸ споделя, че физическото лице Стефан Чолаков също е подал сигнал по случая към Комисията, като е предоставил голям хард диск и допълнителна флаш памет, на която се установява, че има над 33-34 хил. клиента на банката, чиито кредитни досиета са придобити незаконосъобразно и впоследствие публично разпространени.

По решение на КЗЛД⁹ Банка ДСК е глобена с 1 000 000 лева, плащането на които банката не смята да обжалва. Установявайки, че дигиталната система на трезора не е засегната, а течът от банката е в резултат от престъпление – физическа кражба на електронни копия на документи, което не засяга информационните системи, Банката разработва и платформа, в която всеки клиент ще може да провери лично дали неговата информация е била засегната.

Неминуемо след вътрешния одит в Банка ДСК са взети и други мерки, но те не са все още публично достояние.

Въпросът не е приключен, тъй като всеки гражданин, който счита, че правото му на защита на личните данни и неприкосновеност е било нарушено, може да подаде жалба до КЗЛД. Освен това GDPR дава право на всеки, който е претърпял материални или неимуществени вреди в резултат на нарушение на регламента, да получи обезщетение от администратора. „Субектите на данни следва да получат пълно и действително обезщетение за претърпените от тях вреди“, предвижда регламентът (<https://www.bia-bg.com/focus/view/23312/>).

⁸ Заб.: <https://btvnovinite.bg/bulgaria/kzld-globi-s-1-mln-leva-banka-dsk.html>

⁹ Заб.: https://www.cdpd.bg/?p=news_view&aid=1514

Заклучение

От изложеното дотук може да се направят следните изводи:

1. В съвременното общество с развитието на технологиите все повече се увеличават злоупотребите от хакерски атаки, което неминуемо води до насочване на вниманието към разработването на адекватни мерки и процедури за защита.

2. Мерките, които банковите институции вземат през последните години, значително повишават до известна степен ефективността на противодействието им срещу заплахи и намаляват риска от злоупотреби.

3. Същевременно нововъведенията в техническо отношение и съвременните научни достижения работят и в услуга на престъпността. Това прави много трудно предвидимо как, кога и по какъв начин те могат да застрашат някой актив на банкова институция.

4. Необходимо е подобрение, актуализация и въвеждане на по високи изисквания на мерките за контрол в банките и преквалифициране на рисковете с цел минимизиране на възможностите от злоупотреби както на служители, така и на външни за банковите институции лица.

5. Засилване ролята, обхвата и интензивността на предварителния вътрешен контрол в банките.

Използвани източници

Динев, М. (1999). Контрол в социалното осигуряване, София

Тананеев, Е., Крумов, К., Стойкова, П. (2008). Вътрешен контрол и одит в банките. Академично издателство: Свищов.

Томов, Й. (2009). Теория на контрола. Академично издателство: Свищов.

Bowker, Art (2012). The Cybercrime Handbook for Community Corrections: Managing Risk in the 21st Century. Springfield: Thomas

Закон за защита на личните данни. - обн. ДВ, бр.81/2016.

Наредба №10 за вътрешния контрол в банките. - обн. ДВ, бр.102/2006

Наредба за системата от мерки, способности и средства за физическата сигурност на класифицираната информация и за условията и реда за тяхното използване, ПМС№52 / 2003.

<https://www.bia-bg.com/focus/view/23312>

Европейска сметна палата, Единен надзорен механизъм – добър старт, но с необходими допълнителни подобрения, Специализиран доклад №29, 2016.

Николова, Д., Фети, Н. (2019) Защита на личните данни, Издателство: Труд и Право.

Целков, В., Петков, Д., Средов, Г., Георгиев, П. (2019). Защита на данните. Принципи и практики, Издателство: Нова звезда.

[https://dskbank.bg/новини-и-промоции/детайли/2019/08/29/ изявление- на- банка- дск-относно-решение-на-кзлд](https://dskbank.bg/новини-и-промоции/детайли/2019/08/29/изявление-на-банка-дск-относно-решение-на-кзлд)

<https://btvnovinite.bg/bulgaria/kzld-globi-s-1-mln-leva-banka-dsk.html>

https://www.cpdp.bg/?p=news_view&aid=1514

<https://news.bg/finance/banka-dsk-s-globa-ot-1-miliona-leva-zaradi-tech-na-lichni-danni.html>

СТОПАНСКА АКАДЕМИЯ „Д. А. ЦЕНОВ“ - СВИЩОВ

ГОДИШЕН

АЛМАНАХ
НАУЧНИ ИЗСЛЕДВАНИЯ
НА ДОКТОРАНТИ

НАУЧНИ ИЗСЛЕДВАНИЯ
НА ДОКТОРАНТИ

ГОДИШЕН
АЛМАНАХ



Том XII, 2019

Книга 15

Том XII, 2019 г.
Книга 15

Академично издателство
„ЦЕНОВ“ - Свищов

РЕДАКЦИОНЕН СЪВЕТ:

Доц. д-р Стефан Маринов Симеонов – главен редактор

Доц. д-р Росица Христова Колева – зам.главен редактор

Доц. д-р Красимира Борисова Славева – организационен секретар

Доц. д-р Марина Ангелова Николова

Доц. д-р Христо Георгиев Сирашки

Доц. д-р Ваня Григорова

Екип за техническо обслужване:

Анка Петкова Танева – стилев редактор

Ст. преп. Маргарита Евгениева Михайлова – превод и редакция
на английски език

Милена Димитрова Александрова – технически секретар

ISSN 1313-6542

СЪДЪРЖАНИЕ

Студии

Таня Стайкова Йорданова ПОВЕДЕНИЕ НА ДОМАКИНСТВОТА В БЪЛГАРИЯ ПРИ ВЗЕМАНЕ НА РЕШЕНИЯ ЗА СПЕСТЯВАНЕ И ИНВЕСТИРАНЕ	5
Анелия Стефанова Пенева АНАЛИЗ НА ВЗАИМОВРЪЗКИТЕ МЕЖДУ КАПИТАЛОВИТЕ И ВАЛУТНИТЕ ПАЗАРИ	29
Криста Цветанова Нейкова КОНЦЕПТУАЛНИ ОСНОВИ НА ЛОЯЛНОСТТА	51
Борислав Красимиров Киров ЕФЕКТЪТ НА ЕВРОПЕЙСКИТЕ КРЕДИТНИ РЕГУЛАЦИИ ВЪРХУ ИПОТЕЧНОТО КРЕДИТИРАНЕ И ИНВЕСТИЦИИТЕ В ИПОТЕЧНИ ОБЛИГАЦИИ	78
Мариета Бориславова Спасова ПРОГРАМАТА ЗА ОСИГУРЯВАНЕ НА КАЧЕСТВО И УСЪВЪРШЕНСТВАНЕ – ОСНОВА ЗА ПОВИШАВАНЕ КАЧЕСТВОТО НА ВЪТРЕШНИЯ ОДИТ В ПУБЛИЧНИЯ СЕКТОР	98
Михаела Стоянова Монова НОВИТЕ ЗАКОНОДАТЕЛНИТЕ ПРОМЕНИ ПО ЗАСТРАХОВКА „ГРАЖДАНСКА ОТГОВОРНОСТ“ НА АВТОМОБИЛИСТИТЕ И ВЛИЯНИЕТО ИМ ВЪРХУ ФИНАНСОВАТА СТАБИЛНОСТ НА БЪЛГАРСКИЯ ЗАСТРАХОВАТЕЛЕН ПАЗАР	125

Статии

Юлиан Сашков Бенев АНАЛИЗ НА АКТУАЛНИТЕ ПРОБЛЕМИ В БАНКОВАТА СФЕРА И НЕЙНАТА СТРАТЕГИЧЕСКА ОРИЕНТАЦИЯ В КОНТЕКСТА НА ДИГИТАЛИЗАЦИЯТА НА БАНКОВИТЕ УСЛУГИ В ЕС	157
Пресиян Илианов Василев ОРГАНИЗАЦИОННИ ПОДХОДИ ЗА МИНИМАЛИЗИРАНЕ НА КИБЕРРИСКОВЕТЕ ПРИ ОДИТОРСКАТА ДЕЙНОСТ	174

Цветелина Красмирова Иванова НАСОКИ ЗА УСЪВЪРШЕНСТВАНЕ НА ОРГАНИЗАЦИОННАТА КУЛТУРА	190
Димитър Пламенов Попов ИЗСЛЕДВАНЕ НА ОБЕМА И ДИНАМИКАТА НА СЕКЮРИТИЗИРАНИЯ ВЪТРЕШЕН ДЪРЖАВЕН ДЪЛГ НА РЕПУБЛИКА БЪЛГАРИЯ В ПЕРИОДА СЛЕД ПРИСЪЕДИНЯВАНЕТО КЪМ ЕС	213
Пламен Василев Георгиев СЪСТОЯНИЕ И ТЕНДЕНЦИИ В РАЗВИТИЕТО НА БЪЛГАРСКАТА ИКОНОМИКА. ЕФЕКТИ И ЗАПЛАХИ ЗА БАНКОВАТА СИСТЕМА	226
Светла Михайлова Боянова ОТНОСНО ЗНАЧЕНИЕТО НА ВЪТРЕШНИЯ КОНТРОЛ ЗА БАНКОВАТА СИГУРНОСТ	237
Венцислав Георгиев Диков РЕГУЛАТОРНА РАМКА ЗА ФИНАНСОВО-ИКОНОМИЧЕСКА ЗАЩИТА НА АВТОРСКИТЕ ПРАВА В ЕС	266
Муса Мустафа Сръкьов МОДЕЛ ЗА ФИНАНСИРАНЕ НА СРЕДНИТЕ УЧИЛИЩА „БОНУС–ВАУЧЕР“	277
Николай Тодоров Здравков УПРАВЛЕНСКИ ФИНАНСОВ АНАЛИЗ НА ЗАСТРАХОВАТЕЛНИТЕ ПОСРЕДНИЧЕСКИ ФИРМИ - СРАВНИТЕЛЕН АНАЛИЗ НА МОДЕЛИ НА СВОБОДНИТЕ ПАРИЧНИ ПОТОЦИ	285
Таня Иванова Рисемова ПРОБЛЕМИ НА ЗАЕТОСТТА И БЕЗРАБОТИЦАТА В БЪЛГАРСКИТЕ ОБЛАСТИ ПО ТЕЧЕНИЕТО НА ДОЛЕН ДУНАВ	298
Ана Борисова Иванова ИЗТОЧНИЦИ И МОДЕЛИ ЗА ФИНАНСИРАНЕ НА ЗДРАВЕОПАЗВАНЕТО – СПЕЦИФИКА И ЕФЕКТИВНОСТ ПРИ ПРЕДОСТАВЯНЕ НА ЗДРАВНИ УСЛУГИ ...	313
Люба Мартинова Митева КРИТИЧЕН АНАЛИЗ НА ПРОБЛЕМИТЕ В БОЛНИЧНИЯ СЕКТОР	325

Станислав Иванов Шишманов БАНКИТЕ И КАСОВОТО ИЗПЪЛНЕНИЕ НА ДЪРЖАВНИЯ И ОБЩИНСКИТЕ БЮДЖЕТИ	341
Валери Йорданов Велковски ПРОБЛЕМИ НА УСТРОЙСТВЕНИТЕ ПОЛИТИКИ И УСТРОЙСТВЕНИТЕ МЕРОПРИЯТИЯ В ЗЕМЕДЕЛСКИТЕ ЗЕМИ (НА ПРИМЕРА НА ЕМПИРИЧНО ИЗСЛЕДВАНЕ)	355
Симеон Венциславов Симеонов СПЕЦИФИКА НА ТУРИСТА ПРАКТИКУВАЩ КУЛИНАРЕН ТУРИЗЪМ	383
Emre Zafer Güney BUTCHERS SCHEDULING MODEL EXAMINATION BY TIME STUDY OBSERVATIONS	398
Андрей Йорданов ПРЕДИЗВИКАТЕЛСТВАТА ПРЕД ТОВА ДА БЪДЕШ AGILE /SCRUM	408
Диана Христова КОРПОРАТИВНА АМНЕЗИЯ И МОНИТОРИНГ НА НЕЯВНИТЕ ЗНАНИЯ В ОРГАНИЗАЦИИТЕ	416
Борислав Боев ПРОЕКТНОТО УПРАВЛЕНИЕ ПРИ ИЗГРАЖДАНЕТО НА НОВИ ЯДРЕНИ МОЩНОСТИ – ОСОБЕНОСТИ И ПРЕДИЗВИКАТЕЛСТВА	424
Димитър Георгиев Тричков ПАЗАРНИ ПРЕДИЗВИКАТЕЛСТВА И ВЪЗМОЖНОСТИ ПРЕД ТЕЛЕКОМИТЕ В БЪЛГАРИЯ	445
Veneta Todorova Lyubenova BRAND TRUST AS A SOURCE OF BRAND EQUITY	473
Росица Атанасова Проданова ЕВРОПЕЙСКАТА ЦЕНТРАЛНА БАНКА – АНАЛИЗ НА ИНСТИТУЦИЯТА И ПОЗИЦИЯТА Й В СЧЕТОВОДНИЯ БАЛАНС	488
Зорница Крумова ИНОВАЦИИ – ОСНОВЕН ФАКТОР ЗА ПОВИШАВАНЕ НА КОНКУРЕНТОСПОСОБНОСТТА	507
Yaakov Itach FINANCIAL LITERACY LEVEL OF HIGH SCHOOL STUDENTS AND ITS ECONOMIC PATTERNS REFLECTIONS	518

ГОДИШЕН
АЛМАНАХ
НАУЧНИ ИЗСЛЕДВАНИЯ НА ДОКТОРАНТИ
Студии и статии
Том XII – 2019, книга 15

Даден за печат на 28.05.2020 г., излязъл от печат 02.06.2020 г.
Поръчка № 18464; формат 16/70/100; тираж 50

ISSN 1313-6542

Издателство и печат: Академично издателство „Ценов“
Свищов, ул. Градево № 24