ОТНОСНО КИБЕРСИГУРНОСТТА В ПРЕДПРИЯТИЯТА

Д-р Дияна Банкова
Преподавател
Специалност: „Противодействие на престъпността
и опазване на обществения ред”,
Катедра: „Оперативно-издирвателна дейност”,
Академия на МВР
diyanabankova@gmail.com

Авторът иска да изкаже специални благодарности за подкрепата и вдъхновението на колегите от Академията на МВР, както и на служителите в отдел „Киберпрестъпност” към Главна дирекция „Борба с организираната престъпност” (ГДБОП) – гр. София.

Ключови думи:

Кибер сигурност

ИТ одит

Кибер одит

Кибер риск

Финансови отчети

Кибер престъпления

Законодателни реформи

Резюме

Дигитализацията на одиторското досие вече се счита за нещо напълно нормално. Развитието и автоматизацията на процесите в предприятията трябва да бъдат аналогични и за одиторските дружества. Масовите хакерски атаки нанесоха сериозни загуби за обществото. Слабостите на контролите допускат извършването на редица престъпления. За това и одитът на информационните технологии (ИТ) се модифицира в „кибер одит”. Приложението на този вид одит допринася за повишената сигурност на банките и всяка една индустрия, която е зависима от ИТ технологиите. Тези процеси рефлектират и върху финансовата информация. Чрез повишаване на киберсигурността от страна на одиторите и извършване на някои допълнителни процедури могат да бъдат минимизирани някои рискове. В тази връзка са необходими и законодателни инициативи за повишаването на киберсигурността в Република България.

Въведение

С всеки изминал ден рискът от ***киберпрестъпления*** се повишава както в публичния сектор, така и в частния. Основната причина за тяхната реализация може да се обвърже със *слабостите в контролите и контролната среда на информационните технологии (ИТ)* в една институция. Важно е да бъде обърнато внимание от страна на ***дипломираните експерт-счетоводители, регистрираните***

одитори на тези престъпления. В допълнение, масовата дигитализацията на одиторските досиета крие допълнителни рискове от кибер атаки, за които е нужно да бъдат предприети своевременни мерки.

Клиентите, подлежащи на независим финансов одит, непрестанно въвеждат **иновации и дигитализации в своята дейност и е редно одиторите също да притежават познания за тези нововъведения.** Целите на собствениците е да бъдат по-конкурентноспособни и да достигнат до по-добри финансови резултати в края на отчетните периоди. В тази връзка човешкият труд също търпи сериозни промени и все по-често се заменя от иновативни технологии и аутсорсване на процесите. Всяка една индустрия е засегната от тези промени, като това твърдение дава поле за прояви на нов тип престъпления.

Настоящата статия има за **цел** *да представи значението на киберсигурността в предприятията, ИТ одита, кибер одита, начини за превенция срещу киберпрестъпления.*

Това може да се осъществи с изпълнението на следните **задачи**:

- ✓ определяне на рисковете от дигитализацията на одиторското досие;
- ✓ анализиране на значението и приложението на ИТ одита и кибер одита;
- ✓ изграждане на допълнителна култура за киберсигурност с допълнителни тестове;
- ✓ информация относно отговорната институция, отговаряща за киберпрестъпленията в България.

Всички одиторски компании започнаха масова дигитализация на одиторското досие. Това е нормално, тъй като средата дава възможност процесите да бъдат улеснени чрез електронната документация. Въвеждането на софтуери и облачни пространства от одиторите се превърна в неизменна част от одиторските действия. Само че освен положителния аспект, това начинание крие и сериозни рискове, свързани с: изтичането на информация, кибер атаки, загуба на информация и други.

Световно известните международни одиторски компании ***(Big 4)*** като ***KPMG*** също признават и отделят внимание на променящите се тенденции и иновации в одиторската професия. Според тях, „тъй като цифровите иновации напредват, одиторската професия е принудена да ги следва” [1]. Само че този процес е неотложен и трябва да бъде синхронизиран своевременно.

Deloitte [2] споделя мнението, че поради масовите кибер престъпления е необходимо да се извършват стрес-тестове, свързани с киберсигурността. Представена е за пример ***Bank of England***. Освен че подлежи на редица финансови проверки, банката представя и едно добро ниво на киберсигурност.

Компанията ***Pricewaterhouse Coopers (PwC)*** също се аргументира по отношение на кибер рисковете. За нея „кибер-рискът не е просто технологично предизвикателство, това е бизнес приоритет" [3]. Чрез допълнителни услуги е възможно да се осигури желаната сигурност в дигиталния свят.

Сходно е становището и на други компании като ***Ernst & Young (E&Y)***. Акцентират върху настоящето, че представлява *„епоха на трансформацията"*, описана в доклада – *„In a digital world, do you know where your risks are?*[1] [4]. В техните аргументи се посочва изразяването на допълнителна сигурност чрез – ***„cyber audit"***[2]. От своя страна той включва следното:

- ✓ „необходимостта от съзряване на съществуващите процеси за управление на риска от киберсигурност;
- ✓ познания за нови и бързопроменящи се технологии;
- ✓ сложни счетоводни и регулаторни изисквания;
- ✓ бързо променяща се киберсреда, която изисква промени в политиките и процедурите за повишена нужда от специализирани умения и компетенции за идентифициране и смекчаване на рисковете;
- ✓ проактивна оценка на нови и възникващи рискове" [5].

В тази връзка понятието „**кибер одит**" наподобява много на „**ИТ одит**". Важно е да се отразят разликите и приликите между тях. Затова те ще бъдат представени и анализирани в краткото изследване.

Понятието **„кибер одит"** се среща в редица международни източници. Според част от тях се изпълнява, „когато технологичен екип провежда организационен преглед, за да гарантира, че се прилагат правилните и най-актуални процеси" [6]. Извършва се чрез тестове, които да потвърдят, че сигурността на информацията е в съответствие с приложените политики на една компания. Също така се извършват и интервюта с отговарящите за ИТ процесите. Освен това се дава и оценка на ефективността на ефикасността на киберсигурността в компанията.

Други източници, прилагащи и предлагащи услугите на този вид одит във Великобритания, твърдят, че „одитът за киберсигурност е предназначен да представлява цялостен преглед и анализ на ИТ инфраструктурата на бизнеса" [7]. Служи, за да идентифицира заплахи и слабости в кибер пространството. Обърнато е внимание, че при нарушение на *GDPR (Общ регламент за защита на лични данни)* могат да бъдат налагани съществени санкции. С цел превенция чрез имплементирането на одита за киберсигурността кибер нарушенията могат да бъдат минимизирани.

По отношение разграничението на двата вида одит, обвързан с информационните технологии, е нужно да се прави разлика за техните

[1] Превод от англ. език „В дигиталния свят знаете ли къде са скрити рисковете?
[2] Превод от англ. език „кибер одит".

цели. В тази връзка, „макар че киберсигурността е компонент на професията за ИТ, попадайки под този обширен одитен чадър, тя в своята практика попада извън сферата на одита в усилията си да **предотвратява, открива и реагира на заплахи**" [8]. Съществена е разликата, че ИТ одитът е специализиран върху специфичните кибер атаки.

Съществена разлика има и по отношение на необходимите компетенции. За кибер одита е нужна по-голяма компетентност и експертиза в областта на киберсигурността, включително в областта на мрежовото и системно администриране.

Тук е важно да се отбележи, *че ИТ одитът се обвързва пряко и единствено само с ИТ контролите*. Докато при кибер одита обемът от операции е значително по-голям и сложен, но изисква и познания в областта на одита. Това също се отразява и в заплащането. Например, „докато инженерите по киберсигурност, анализаторите на киберсигурността и архитектите за киберсигурност могат да спечелят между 95 000 – 210 000 долара, професионалистите, работещи в сферата на одита, ще се приберат вкъщи със сумата между 65 000 – 110 000 долара" [9].

Тези специфични процеси по киберсигурност могат да бъдат обяснени като съвкупност от умения между одита на информацията и киберсигурността. Целите и на двата вида одит е *да осигурят защита*. Но каква е разликата помежду им?

Според **Leonard Coronel** целите на ИТ одитите са насочени върху инфраструктурата на едно дружество. Функцията на „ИТ одиторите е да правят оценка на физическото присъствие, като разбират съществуващата структура за вътрешен контрол, за да сведат до минимум бизнес риска, който включва прилагането на всички регулаторни изисквания" [10].

Докато мнението на гореспоменатия експерт за „анализаторите на киберсигурност е да изследват същите области, въпреки това те гледат на тях чрез различна цел на предотвратяване и защита на системите на компанията, физически и електронно" [11], действията им се изразяват в извършването на мониторинг и тестове.

След като се представи значението и на двата вида одит, ще бъде отразено поради какви причини тези одити са значими и за финансовите одитори. Често пъти компаниите са атакувани от хакери и се нанасят значителни финансови щети за тях и потребителите на услугите им. За да бъдат сведени до минимално ниво тези рискове, е от значение как функционират: *вътрешният контрол, вътрешният одит и независимият финансов одит*.

Защо кибератаките биха повлияли и на финансовия одит? Защото „те взаимно си влияят и взаимодействат" [12] (Динева: 2014, 61). Изхожда се от твърдението, че финансовите одитори проверяват представените данни в годишните финансови отчети, които са почти изцяло дигитализирани. Важно е да се изследват и рисковете, свързани

с киберсигурността и достоверността на информацията, върху която се базира финансовият отчет.

Човечеството е изправено пред едно огромно предизвикателство – киберпрестъпността, с което трябва да се бори. Към днешна дата това е една от най-големите заплахи за всяка една компания. Като доказателство за тези твърдения ще бъдат представени статистически данни.

Компанията ***Cybersecurity Ventures*** [13] прогнозира, че през 2013 година глобалните разходи, свързани с киберпрестъпността, са 100 милиарда долара, като през 2015 година се увеличават до 400 милиарда долара. Същите разходи през 2017 година възлизат на 1 трилион долара. Прогнозните стойности към 2021 година са 6 трилиона долара.

Тези данни индикират за сериозността на този тип престъпност. Загубите от тази престъпна дейност са значително по-големи дори от считаните за по-сериозни престъпления като трафик на хора, наркотици, оръжия и т.н. Разходите за киберпрестъпност се свързват с:

- ✓ „повреда и унищожаване на данни;
- ✓ откраднати пари;
- ✓ загуба от производителност;
- ✓ кражба на интелектуална собственост;
- ✓ кражба на лични и финансови данни;
- ✓ присвояване;
- ✓ измами;
- ✓ прекъсване на дейността след атака;
- ✓ съдебни разследвания;
- ✓ възстановяване и изтриване на данни и системи от хакери;
- ✓ вреди на репутацията" [14].

Поради всичко, упоменато по-горе, е важно от страна на регистрираните одитори нивото на тези рискове да бъде минимизирано. Одиторите са обвързани, защото разчитат до голяма част на автоматизацията на обработката на данни. Когато „една компания се счита за международна, тя е изправена пред по-голям" [15] (Georgieva: 2019:1) риск от загуба на информация. Особено когато става въпрос за масив на данни в банките и банковите институции. Най-съществени рискове „върху банковата система са: кредитен риск, операционен риск, ликвиден риск и пазарен риск" [16] (Филипова-Сланчева: 2018, 218), включително и ***кибер риск***.

Пример за изградена функционираща рамка за киберсигурност в банковата сфера е политиката на Турция. В изследването *„Audit Techniques For Protecting Against Cyber Attacks: A Bilateral Approach Of Case Studies and Interview"*[17] се представя информация за държавния

регулатор, който осъществява проучвания относно киберсигурността на банките в Турция - *Banking Regulation and Supervision Agency (BRSA).*

Изведени са сведения от *Reuters Istanbul* [18] за нанесените кибератаки върху някои банки и ***SWIFT***[3] кодовете им. Например атаката през 2016 година към **Akbank** е на стойност 4 милиона евро. В допълнение към вече мрачните краски е представена и информация за извършване на хакерски трансфер чрез откраднати права на ***Bangladesh Bank,*** за да се извърши прехвърляне на близо 1 милиард долара от кореспондиращи сметки в САЩ.

Представеният пример изразява сериозността относно необходимостта от кибер одит. Само че този пример е аналогичен и за всяка друга индустрия, основаваща се на дигиталните технологии – застраховане, болници и лечебни заведения и други. За да бъде достоверен финансовият одит, се извършват тестове на оперативната ефективност на контролите. Само че когато сигурността на ИТ в едно дружество е нарушена, аналогично е, че и одиторските становища ще бъдат грешни.

В някои страни вече са взети предвид тези рискове. Например в САЩ от отговорната институция, осъществяваща надзор над одиторската професия – *Public Company Accounting Oversight Board (PCAOB)* [19], е споделено и становище във връзка с киберсигурността и финансовия одит. Отразени са и насоките на *Security Exchange Commision (SEC)* [20] срещу кибератаките.

Нормативната рамка на киберсигурността започва и своята стандартизация. През 2018 година са издадени стандарти от *National Institute of Standards and Technology (NIST) – Framework for Improving Critical Infrastructure Cybersecurity*. Анализирани са ИТ контролите и значението на одиторската дейност в дружествата.

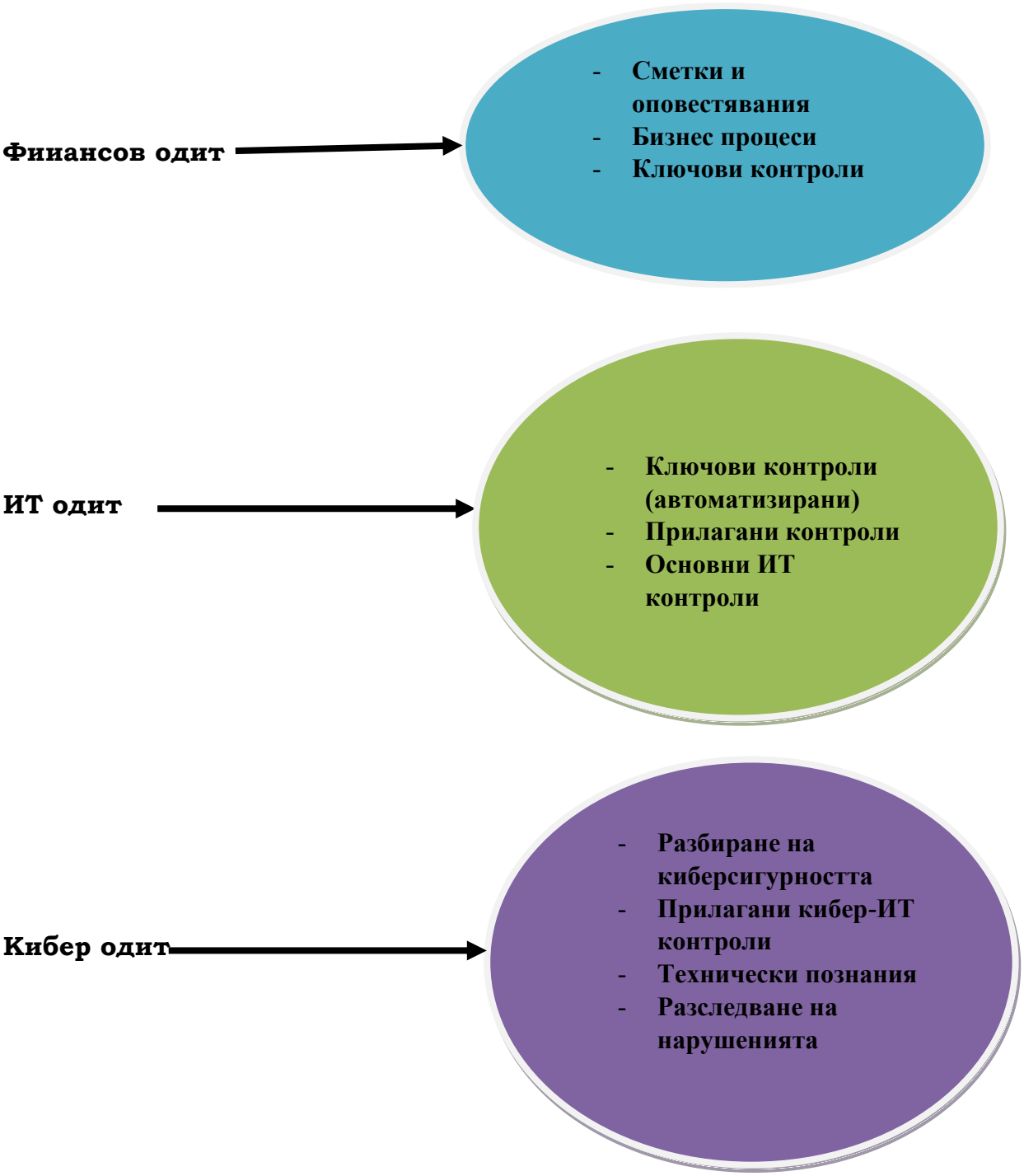
Освен това *The American Institute of Certified Public Accountants (AICPA)* също издава насоки [21], свързани с кибер рисковете. Въвежда се и нов модел през 2017 година – ***„System and Organization Controls" (SOC)*** [22] в одиторската практика, представляващ система за организационен контрол, който обхваща киберсигурността. Чрез него одиторите управляват риска от кибератаки в цялата организация.

Овладяването на кибератаките продължава и в Европейския съюз (ЕС). С имплементирането на *Директива (ЕС) 2016/ 1148 на Европейския парламент и на Съвета относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза* се въвежда регулация, свързана с кибератаките. Тенденцията продължава и развитието си в одиторската професия.

От краткия анализ е важно е да се обобщят и разграничат приложенията на различните одити, свързани с киберпрестъпленията. Затова на следващата фигура ще бъдат представени.

[3] Международна разплащателна система.

Фигура № 1. Разграничение на видовете одит, свързани с кибер рисковете



Източник: *Cyber Security: A Paradigm Shift in IT Auding, Door: M. van Veen* [23]

На фигурата са представени и обобщени дейностите, които извършват финансовият, ИТ и кибер одит. Първият вид одит се свързва с финансовата информация. Чрез него се извършват проверки и тестове на счетоводните записи, бизнес процесите и ключовите контроли на едно дружество.

За повишаване на сигурността се извършва и ИТ одит на контролите. За да бъдат защитени интересите на инвеститорите и на обществото, е важно да бъде минимизирана изкривяваната информация. Съответно поради тази причина се извършва и т.нар „**ИТ одит**”. В този ред на мисли, „казано накратко, необходим е контрол преди събитието, контрол, който активно отстранява условията, които предизвикват отклоненията” [24] (Динев: 2015, 37).

В допълнение могат да се използват и от компаниите и държавното управление одиторите, извършващи превантивен контрол от кибератаки, т. нар. **„кибер одит”**. Макар и чрез дигитализацията на одиторското досие да бъде улеснена дейността на одиторите, това крие допълнителни рискове по отношение на сигурността на информацията в тях. Освен проследяването на неоторизиран достъп до информацията на даден клиент се проверява и непрестанно сигурността на софтуерите в дадено предприятие. Тази дейност изисква и специфични познания и компетенции в кибер областта.

Причините за трансформацията на одиторската професия се свързват с това да се намалят рисковете от измами и пораждащите се нови престъпления. Например въвеждането на различни валути е типично проявление на гореизложеното. В частност на киберпрестъпността.

Експертите в тази област твърдят, че „пробивът в сигурността на онлайн финансовите инструменти води до спад в доверието на финансовите институции и тяхната способност активно да защитават потребителите си” [25] (Колев: 2018, 5). Съответно, за да се повиши доверието на обществото, е необходимо и нивото на киберсигурност от страна на правителството и частния сектор да бъде повишено.

Сривът на ***Търговския регистър (ТР)*** задълбочи тези съмнения. „Въпросният регистър, поддържан от Агенцията по вписванията” [26] (Михов, 2018: 71), нанесе многожество неудобства за обществото поради не добре управлявания кибер риск. Изтичането на личните данни на значителен брой хора от платформата на ***Национална агенция за приходите (НАП)*** затвърждава общественото недоверие в правителството.

Без да се генерализира, тези слабости в държавното управление рефлектират на извършването и на други деяния. Например „терминът изпиране/пране на пари ”, появил се в началото на XX век” [27] (Янев: 2011, 7), вече чрез криптовалутите се осъществява в пъти по-лесно. Налични са „съмнения, че те са финансови пирамиди в модерен технологичен вариант” [28] (Вейсел: 2018,131). Така също могат да бъдат финансирани и други видове престъпления като: тероризъм, трафик на хора, органи, оръжия. Слабостите в контролите, „злоупотреба с власт, била тя икономическа, политическа, административна или съдебна” [29] (Станева: 2018, 32), водят до реализацията на тези престъпления. Затова е от съществено значение да бъдат наблюдавани и проследявани от страна на одиторите нетипичните трансакции и кибер рисковете.

В допълнение, „одиторът няма задължение да разследва измамата" [30] (Пейчева: 2019, 16), но има ангажимент да докладва пред правораздавателните органи – ***Държавна агенция национална сигурност (ДАНС)***. Само че киберпрестъпленията са тясно специализирани. Единствената и основна институция за разкриването и противодействието на киберпрестъпленията е ***отдел „Киберпрестъпност"*** на *Главна дирекция за борба с организираната престъпност (ГДБОП)* към *Министерството на вътрешните работи (МВР).* Морален и професионален дълг е от страна на дипломираните експерт-счетоводители да подават сигнали към съответната институцията, ако забележат съмнителни трансакции и действия, обвързани с кибер пространството.

Спрямо доклада – *„Building Trust in the Digital Age: Rethinking Privacy, Property and Security"* на *Institute of Chartered Accountants in England and Wales (ICAEW),* информационните технологии променят изцяло традиционния начин на работа на компаниите. Затова е от значение финансовите одитори да се фокусират върху някои допълнителни рискове, за да бъдат избегнати бъдещи загуби. Като най-съществени са: „нарушенията на данните и растеж на кибератаки; кражба на самоличност, фишинг имейли, спам и компютърни вируси; противоречиво използване на лична информация; интелектуална собственост и предотвратяване на използването на други от тях"[31].

Поради тези причини е желателно да бъдат извършени допълнителни тестове от одиторите. За допълнителна сигурност на проверяваната компания и за извършващия проверката може да се разработи въпросник. В ***Приложение № 1*** е разработен **примерен** въпросник, свързан с киберсигурността на една компания.

Приложение № 1. Въпросник относно информационната сигурност

Въпроси:	**Бележки:**
Как клиентът определя своите приоритети за сигурност?	
Какви инструменти и инвестиции използва ръководството във връзка със сигурността?	
Как се идентифицират активите на данни и сравняват тяхната важност и чувствителност на информацията?	
Как се насърчава комуникацията на целите и приоритетите за сигурност?	
Как информационните рискове са интегрирани в по-широката рамка за бизнес риска?	
Какви умения и възможности са необходими за ефективното прилагане	

на мерките за сигурност?	
Как могат да се разберат и управляват рисковете за информация на доставчиците на трети страни?	
Какви техники се използват за управление и удостоверяване на самоличността?	
Извършва ли се одит на информационната сигурност в предприятието?	
Имплементирани ли са корпоративни информационни политики?	
Как предприятията приравняват информационните политики с бизнес целите?	
Как дружеството интегрира ползите и рисковете, свързани с ИТ?	
На какъв етап се вземат предвид информационните политики при разработването на нови системи или процеси в рамките на дружеството?	
Какви политики за поверителност се упражняват при международни комуникации?	
Кой поддържа ефективното управление на въпросите, свързани с поверителността?	
Какви методи и подходи упражнява дружеството за комуникацията с потребителите относно третирането на тяхната лична информация?	
Какви специфични технологии се използват от дружеството за повишаване на поверителността на информацията?	
Как компанията събира и управлява съгласието на своите клиенти за обработка на лична информация?	
Дата:	**Изготвил: .....**

Източник: ICAEW, Information Technology Faculty, Building Trust in the Digital Age: Rethinking Privacy, Property and Security, London,UK, 2011, p. 88.

Това са само примерни въпроси, които могат да помогнат на одиторите по отношение на ИТ контролите и киберсигурността в едно дружество. Могат да бъдат актуализирани спрямо дейността на клиента. Все още в България няма издадени насоки в това отношение.

Въпреки че целта на кибер одита е да не допусне нарушения във функциониращия бизнес и държавното управление, за съжаление „юридическата уредба на оперативно-издирвателната дейност, от която се очакват проактивни резултати в борбата с престъпността" [32] (Пенев: 2017,13), свързана с киберпрестъпността, е изключително бедна към този момент. Необходими са законодателни реформи, за да бъдат намалени киберпрестъпленията.

От гореизложените анализи могат да се обобщят следните по-важни **изводи**:

- ✓ Инвестицията в киберсигурността е важна и за одиторските дружества. По този начин ще бъдат защитени интересите на потребителите на този вид услуги.
- ✓ *ИТ одита* служи само за тестове на контролите в едно дружество и не изисква специфични компетенции в областта на киберсигурността.
- ✓ *Кибер одит* – служи за допълнителна сигурност, за да намали рисковете от кибер атаки или други мероприятия, свързани с финансови загуби. Изисква допълнителни компетенции в ИТ сферата, както и познания в областта на одита.
- ✓ Представен е *примерен* въпросник, свързан с киберсигурността в едно дружество, който може да се приложи от одиторите в одиторското досие;
- ✓ Инициране на *законодателни реформи* в областта на киберсигурността.

Нарастващата киберпрестъпност дава отражение и върху финансовите резултати на компаниите. Все повече средства започват да се инвестират в киберсигурността. Дигитализирането на одиторското досие изисква също допълнителни инвестиции за гарантиране на сигурност и конфиденциалност на информацията на клиентите. Тези иновации се припокриват и в самият одит. Тенденциите изискват трансформацията на ИТ одита в разширение до кибер одит, който да минимизира рисковете от хакерски атаки. По този начин и финансовата информация ще бъде по-достоверна. Необходими са законодателни инициативи за повишаване на сигурността в държавното управление, както и в бизнеса.

Библиографска справка:

1. *Mark Meuldijk. Audit Committee News, Edition 58/Q3 2017/Focus on Audit Quality, Impact of digitization on the audit profession, KPMG International, p. 34.*

2. *Staying Relevant, 2020 Hot Topics for IT Internal Audit in Financial Services, Report, 2019 Deloitte LLP, Creative Services.*
3. *Cyber security and Privacy: Managing cyber risks in an interconnected world, <https://www.pwc.com/m1/en/services/assurance/risk-assurance/cyber-security.html>, last available on: 11.01.2020/6:20 p.m.*
4. *EY. In a digital world, do you know where your risks are?, <https://www.ey.com/Publication/vwLUAssets/EY-in-a-digital-world-do-you-know-where-your-risks-are-sa-final/$FILE/EY-In-a-digital-world-do-you-know-where-your-risks-are-sa-final.pdf>, last available on: 13.01.2020/8:20 p.m.*
5. *Ibid, p. 16.*
6. *What is cyber audit? <https://www.quora.com/What-is-cyber-audit>, last available on: 14.01.2020/5:20 p.m.*
7. *Cyber Security Audit, <https://cyfor.co.uk/cyber-security/cyber-security-audit/>, last available on: 12.01.2020/1:20 p.m.*
8. *IT Audit vs Cyber Security, Published 18 May 2018, <https://www.careersincyber.com/article-details/5/it-audit-v-cyber-security/>, last available on: 13.01.2020/9:20 p.m.*
9. *Ibid.*
10. *Moving from IT Audit to Cyber security, Published: 28 Jun 2016, <https://www.careersinaudit.com/article/moving-from-it-audit-to-cyber-security/>, last available on: 11.01.2020/3:20 p.m.*
11. *Ibid.*
12. *Dineva, V. (2014). Metodologicheski aspekti na vatreshnia odit (izsledvane v zastrahovatelnia sector). Sofia: IK ATL-50 [Динева, В. 2014. Методологически аспекти на вътрешния одит (изследване в застрахователния сектор). София: ИК АТЛ-50]*
13. *Cyber Security: A Paradigm Shift in IT Auditing, M. van Veen, <https://www.compact.nl/articles/cyber-security-a-paradigm-shift-in-it-auditing/#ref> last available on: 10.01.2020/2:20 p.m.*
14. *Ibid.*
15. *Georgieva, D. (2019). Mandatory and Voluntary R&D Data Disclosure: Evidence from Bulgaria, Academy of Accounting and Financial Studies Journal, Volume 23, Issue 5.*
16. *Filipova-Slancheva, A. (2018). Finansovi otcheti na bankite – reglamenti i analizi. Sofia: IK-UNSS [Филипова-Сланчева, А. 2018. Финансови отчети на банките – регламенти и анализи. София: ИК-УНСС].*
17. *Kizil, Cevdet and Doğan, Emine, Audit Techniques for Protecting Against Cyber Attacks: A Bilateral Approach of Case Studies and Interview (December 20, 2017). Dorien DeTombe, Gerhard-Wilhelm Weber and Semih Kuter (Eds.), Societal Complexity, Data Mining and Gaming, State-of-the-Art 2017, Amsterdam Europe: Greenhill &*

Waterfront. Version: 001, ISBN/EAN: 978-90-77171-54-7. pp. 125-135.

18. *Turkey's Akbank faces $4 million hit from attempted cyber heist, Can Sezer, Birsen Altayli, <https://www.reuters.com/article/us-akbank-cyber-idUSKBN1450MC>, last available on: 09.01.2020/3:20 p.m.*
19. *PCAOB, Standing Advisory Group Meeting Panel, Discussion – Cybersecurity, June 5-6, 2018, <https://pcaobus.org/News/Events/Documents/Cybersecurity%20Briefing%20Paper.pdf>, last available on: 10.01.2020/9:20 a.m.*
20. *The Securities and Exchange Commission (the "Commission") is publishing interpretive guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents, <https://www.sec.gov/rules/interp/2018/33-10459.pdf>, last available on: 10.01.2020/10:20 a.m.*
21. *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 National Institute of Standards and Technology April 16, 2018, <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>, last available on: 10.01.2020/9:10 a.m.*
22. *System and Organization Controls: SOC Suite of Services, <https://www.aicpa.org/SOC>, last available on: 10.01.2020/2:20 p.m.*
23. *Cyber Security: A Paradigm Shift in IT Auditing, M. van Veen, <https://www.compact.nl/articles/cyber-security-a-paradigm-shift-in-it-auditing/#ref>, last available on: 11.01.2020/3:20 p.m.*
24. *Dinev, M. (2015) Kontrol i regulirane v socialnoto upravlenie, Sofia: IK-UNSS [Михаил, Д. 2015. Контрол и регулиране в социалното управление. София – ИК-УНСС].*
25. *Kolev, Ya. (2018) Protivodejstvie na finansovite kiberprestuplenia v Bulgaria. Digitalni izmami i kibersigurnost. Sofia: IK-UNSS [Колев, Я. 2018. Противодействие на финансовите и киберпрестъпления в България. Дигитални измами и киберсигурност. София– ИК-УНСС].*
26. *Mihov, S. (2018) Informatsia ot yavni iztochnitsi za nuzhdite na operativno-izdirvatelnata deynost Visshe uchilishte po sigurnost i ikonomika, TOM XV. Plovdiv: IK-VUSI [Михов, С. 2018. Информация от явни източници за нуждите на оперативно-издирвателната дейност. Висше училище по сигурност и икономика. Том XV. Пловдив: ИК-ВУСИ].*
27. *Yanev, R. (2011). Protivodeystvie na izpiraneto na pari. Sofia: AMVR [Янев, Р. 2011. Противодействие на изпирането на пари. София: АМВР].*
28. *Veysel, A. (2018). Schetovodni aspekti na kriptovalutite. Digitalni izmami i kibersigurnost. Sofia: IK-UNSS [Вейсел, А., 2018.Счетоводни аспекти на криптовалутите. Дигитални измами и киберсигурност. София: ИК-УНСС]*

29. *Staneva, V. (2018). Finansovo-schetovodni aspekti na antikoruptsiyata. Mezhdunaroden diskusionen forum „Obrazovanie, nauka, inovatsii“, Obshtestvo, antikoruptsia, administratsia. Sofia: Nyuans dizayn, ISBN: 978-954-8655-68-2 [Станева, В. 2018. Финансово-счетоводни аспекти на антикорупцията. Международен дискусионен форум „Образование, наука, иновации“, Общество, антикорупция, администрация. София: Нюанс дизайн, ISBN: 978-954-8655-68-2.]*

30. *Peycheva, M. (2019). Izmami, riskove i cherveni flagove v oblastta na choveshkite resursi. Sofia: IK ATL-50 [Пейчева, М. 2019. Измами, рискове и червени флаговев областта на човешките ресурси. София: ИК АТЛ-50].*

31. *Building Trust in the Digital Age: Rethinking Privacy, Property and Security", Institute of Chartered Accountants in England and Wales, Report, November 2011.*

32. *Penev. Y. (2017). Proaktivno kriminalno razsledvane. Sofia: AMVR biuletin 37 [Пенев, Й. 2017. Проактивно криминално разследване. София. Бюлетин 37: АМВР].*

33. *Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета относно мерки за високо общо ниво на сигурност на мрежите и информационните системи.*

ABOUT CYBERSECURITY IN THE COMPANIES

Diyana Bankova**, **PhD
Visiting Professor
Academy of the Ministry of Interior

Keywords:

Cyber security

IT audit

Cyber audit

Cyber risk

Financial statements

Cyber crimes

Legislative reforms

Summary

Digitization of the audit files is considered to be completely normal. The development and automation of company processes should be similar for audit companies. Massive hacking attacks have caused serious losses to the public interests. The abuse of weaknesses in controls allows numbers of crimes to be committed. That is why the Information Technology (IT) audit is being modified into a cyber audit. The application of this type of audit contributes to the increased security of banks and any industry that is dependent on IT technologies. These processes also affect financial information. Increasing cybersecurity by auditors and performing some additional procedures can minimize some risks. In this regard, legislative initiatives are also needed to improve cybersecurity in the Republic of Bulgaria.