ОРГАНИЗАЦИОННИ ПОДХОДИ ЗА МИНИМАЛИЗИРАНЕ НА КИБЕРРИСКОВЕТЕ ПРИ ОДИТОРСКАТА ДЕЙНОСТ[1]

Пресиян Илианов Василев
Стопанска академия „Д. А. Ценов“ – Свищов
Катедра „Контрол и анализ на стопанската дейност“
e-mail: d010117190@uni-svishtov.bg

Резюме: Условията на дигитализиране и компютъризиране на процесите и дейностите налагат, одитът да се приспособява към тях чрез прилагане на адекватни и иновативни подходи. Тези условия пораждат нови заплахи и предизвикателства, свързани с кибератаки. Нанесените финансови и репутационни щети от последните се увеличават всяка година. Напредъкът в технологиите осигурява конкурентни предимства на организациите и одиторите, но изисква повече усилия и концентриране на вниманието към управлението на киберриска. Целта на разработка е да се представи влиянието на технологиите върху одитната дейност. В резултат на направените анализи са изведени организационните подходи, прилагани от одиторите, с цел минимализиране на възникналите заплахи. Във връзка с това е посочен авторов модел, чиято цел е оценка на киберриска.

Ключови думи: одит, оценка на риска, киберриск, подходи
JEL: M42, O33.

ORGANIZATIONAL APPROACHES TO MINIMIZE CYBER RISK IN AUDIT ACTIVITIES

Presian Ilianov Vasilev
D. A. Tsenov Academy of Economics – Svishtov
Department of Control and Analysis of Economic Activity
e-mail: d010117190@uni-svishtov.bg

Abstract: The conditions of digitalization and computerization of processes and activities require a corresponding adaptation of audit by applying adequate and innovative approaches. These conditions create new threats and challenges related to cyber-attacks. The financial and reputational damage caused by the latter has been increasing every year. Advances in technology provide for competitive advantages for organizations and auditors, but require greater effort and focus on cyber risk management. The aim of the paper is to present the impact of technology on audit activity. The paper features the organizational approaches auditors apply to minimize the related threads and proposes an original model to assess cyber risk.

Keywords: audit, risk assessment, cyber risk, approaches.
JEL: M42, O33

[1] Разработката е отличена с 1-во място в секция „Счетоводство, контрол, отрасли, мениджмънт, маркетинг, туризъм“.

Въведение

Работата в киберсреда и използването на иновативни, съвременни технологии пораждат актуализиране на организационните подходи при одитния процес. Във връзка с тези предизвикателства при одита се осъществяват промени, касаещи модификация в начина на осъществяване на процесите и оценката на риска. Тази модификация е свързана с придобиване на нови знания и умения относно киберсигурност, оценка на критични точки в информационната инфраструктура, предотвратяване на опити за отдалечен достъп до чувствителна информация, възможни начини за проникване в системата, оценка не само на традиционния риск, но и на киберриска. Развитието на технологиите предоставя на извършителите на неправомерни действия нови възможности за атака, но същевременно помага на организациите и одиторите да изградят по-усъвършенствани стратегии за превенция и разкриване на новите заплахи и рискове.

Основната **цел** на настоящата разработка е да се представи влиянието на киберрисковете при технологиите върху одитната дейност. Въз основа на анализа са очертани основните рискове от прилагането им в одита.

Поставената цел се реализира посредством изпълнение на следните **задачи**:

- проследяване влиянието на киберрисковете върху одиторската дейност при работа в киберсреда;
- извеждане на основните организационни подходи, използвани за минимализиране на киберрисковете.

Обект на изследване е изменението в подходите, използвани от одитора, съобразно промените в резултат на дигитализация и компютъризация на системите.

Предмет на настоящата разработка е взаимовръзката между използваните технологии, новите рискове и заплахите от дигитализацията на процесите в организациите и необходимостта от адаптиране на подходите в одита към новите условия.

1. Рискове на киберсреда и влиянието им върху одиторската дейност

С развитието на технологиите и внедряването им в цялостния процес на работа в организациите на преден план се появяват нови ***заплахи и предизвикателства, свързани с оценка на киберрисковете.*** Като следствие използваните до този момент механизми и подходи се налага да бъдат осъвременени и усъвършенствани. Едновременно с това контролните органи е необходимо да актуализират знанията, уменията и компетенциите си, за да бъдат в помощ на организациите, към които принадлежат.

Киберрискът представлява *„риск, свързан с използването на компютърен хардуер и софтуер както в локални мрежи, така и в глобалната мрежа, в системи за сетълмент и разплащане, системи за електронна търговия, както и риска, свързан с натрупването, съхранението и използването на лични данни“* (Онищенко & Кирбаба, 2017). Това означава, че този вид риск е част от почти всяка система или дейност, която може да се реализира, вследствие на което този риск е възможно да има негативно отражение върху одиторската дейност и осъществяваните одиторски процедури.

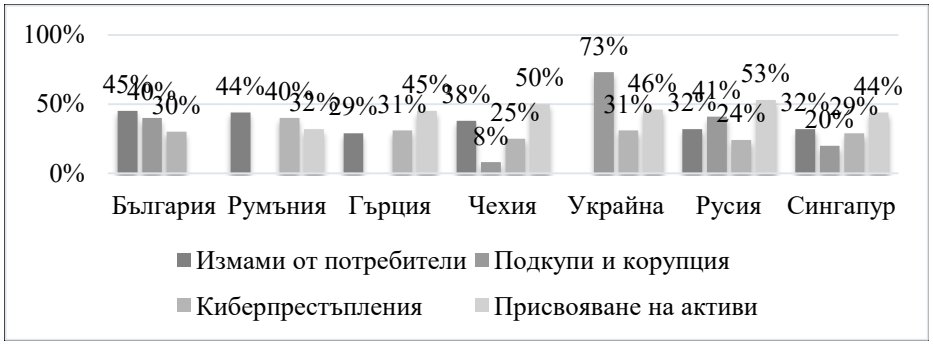
Съществува друга дефиниция за понятието „киберриск“ - *„рискът да се понесат загуби и/или да се извършат допълнителни разходи, поради незаконни действия на трети страни, чрез използване на компютърни и информационни системи или мрежи“* (Инструкцию об организации системы управления рисками в банках, 2018). Киберрискът възниква в резултат на използване на онлайн мрежи или комуникационни системи, като основната му ***цел е получаване на неправомерен достъп до конкретна информация, система или информационни потоци посредством „въвеждане“ на зловреден софтуер.***

Ролята на одиторите е да категоризират риска в организацията, т.е. нисък, среден или висок, след което да преценят до каква степен този риск е съществен и какво влияние може да окаже върху дейността на организацията. При редица компании служителите все повече се налагат да работят в киберсреда. Поради това нуждата от обучения, свързани с кибер-сигурност, оценка на критични точки в информационната инфраструктура, възможности за отдалечен достъп до „чувствителна информация“, начини за проникване в системата, нараства. ***Именно чрез независимата и обективната си оценка одиторите могат да дадат разумна степен на сигурност, че политиките и процедурите, свързани със сигурността, се изпълняват съобразно предварително определения план***.

Във връзка с това одиторите, независимо външни или вътрешни, трябва да заложат в **своя одитен план оценка на риска, но не само на традиционния риск, но и на дигиталния (кибер) риск.** Необходимо е да се изгради стратегия за сигурност, в която да се включи ***създаването или обновяването на система за ранно сигнализиране на проблемни области***, която да е обвързана с програма за обучения, с акцент – придобиване на знания в областта на киберрисковете и сигурността.

В подкрепа на изложеното е посочено осъщественото изследване на PricewaterhouseCoopers (PwC), свързано с основните икономически престъпления, установени в Централна и Източна Европа (ЦИЕ), Балканския полуостров и една от развитите страни – Сингапур за 2018 г.:[2]

[2] *Забележка:* За България, Румъния, Гърция и Украйна липсват данни за определени икономически престъпения, поради факта, че в проучванията за тези страни не са посочени данни.



Адаптирано от източник: (Сындби & Мамасян, 2018), (Novikova, Muller, Vostrova, Ulyakin, & Wood, 2018), (Perris & Pikis, 2018), (Klimczak , Chuprykov , & Turczyn , 2018), (Qureshi, Chirita, Jankech, & Dosedělová, 2018), (Sundbye & Sebov, 2018), (Tek, et al., 2018)

Фигура 1. Видове икономически престъпления в страните от ЦИЕ, Балканския полуостров и развитите страни, 2018 г.

Данните от фигурата са показателни, че в голяма част от случаите основният риск е киберпрестъплението. При част от страните то е на трето място – България (30%), Чехия (25%), Украйна (31%) и Сингапур (29%). В останалите случаи този вид престъпления са на второ място – Румъния (40%) и Гърция (31%), единствено в Русия са на четвърто място с 24%. Значителният относителен дял налага адаптиране на организацията на одитната дейност към новите заплахи чрез използване на съвременни подходи и механизми за ограничаването им.

В същото проучване на PwC се посочва, че за *последните две години киберпрестъпленията са се придвижили до третото място на най-често срещаните икономически престъпления в България*, *като заемат 30% относителен дял* (Сындби & Мамасян, 2018, стр. 9). В световен мащаб *киберпрестъпленията са нанесли щети на обществото в размер на над 3 трилиона долара за 2015 г. и се очаква през 2021 г. те да нараснат до 6 трилиона долара годишно на база направеното предположение на Cybersecurity Ventures* (Morgan, 2019, p. 3). Данните доказват значимостта и осезателния ефект, който оказват тези неправомерни действия не само върху отделните държави, но и в световен мащаб.

Във връзка с това същността на киберпрестъпленията се свързва с това, че те са „*действия, насочени срещу поверителността, целостта и наличността на компютърните системи, мрежи и компютърните данни, както и злоупотреба с такива се възприема като криминално поведение и се търси съответното наказателно преследване“* (Council of Europe, 2001). За Стойкова те *„имат характеристиката на инкриминирани противоправни деяния, които са извършени в киберпространството, използват интернет среда и/или са подпомогнати от наличието на интернет. При тях се реализират вреди както на физически, така и на юридически лица“* (Stoykova, 2012, p. 634).

От дефинициите може да се обобщи, че киберпрестъпленията ***са общественоопасни действия или бездействия, които включват използването на компютър с цел извличане на лична информация (пароли, финансова информация, кражба на самоличност и др.) и използването ѝ с цел увреждане и/или злоупотреба.*** Тези неправомерни действия оказват негативно отражение главно на няколко ***критични зони като здравеопазване, транспорт, включително и от финансовия сектор*** (European Union Agency for Law Enforcement Cooperation, 2018, p. 16).

Показателно за адаптирането на ръководителите на организациите към работата в киберсреда е изследването на Harvey Nash/KPMG, според което *26% от IT-лидерите са „много добре“ подготвени за кибератаки* (Ellis & Bates , 2019). Това означава, че лидерите се чувстват все по-уверени, че могат да преодолеят и да се справят с този риск (в сравнение през 2018 г. е 22%, 2017 г. – 21%, 2016 г. – 22%). **При работа в киберсреда основна роля имат не толкова персоналният компютър или програмите, които се използват, а човешкият фактор.** Вследствие на това е наложително да се проследят прилаганите организационни подходи с цел минимализиране на възникналите кибер заплахи.

2. Одитни подходи в отговор на идентифицираните киберрискове

Придобиването на разбиране за предприятието и неговата среда е съществен аспект при изпълнението на одит. Чрез това разбиране се установяват отправни основни критерии, в обхвата на които одиторът планира одита и упражнява професионална преценка за оценяване на рисковете, както и начините за отговор по отношение на тези рискове. Във връзка с това от ***изследването на Ernst & Young са изведени най-големите заплахи за организацията и най-ценната информация за извършителите на неправомерния деяния***:

Таблица 1
Топ 10 на най-големите заплахи за организацията

Вид заплаха	Случаи (процент)
Фишинг	22%
Малуеър	20%
Кибератака (с цел влошаване на работата)	13%
Кибератака (с цел кражба на пари)	12%
Измама	10%
Кибератака (с цел кражба на IP адрес)	8%
Спам	6%
Вътрешни атаки	5%
Природни бедствия	2%
Шпиониране	2%

Източник: (van Kessel, et al., 2018, p. 9).

На база данните може да се обобщи, че най-честите заплахи са от фишинг (22%), малуеър (зловреден софтуер) – 20% и кибератака с цел влошаване работата на организацията 13%. ***Най-разпознаваемите неправомерни действия като спам, измама и шпиониране са на заден план, т.е. не са толкова често използвани като средство за достигане до чувствителни данни и информация. Съответно те са най-малко като процент случаи – 6%, 10% и 2%***.

Най-ценните данни за извършителите на неправомерни действия са информацията за клиентите, финансовата информация и стратегическите планове (вж. табл. 2).

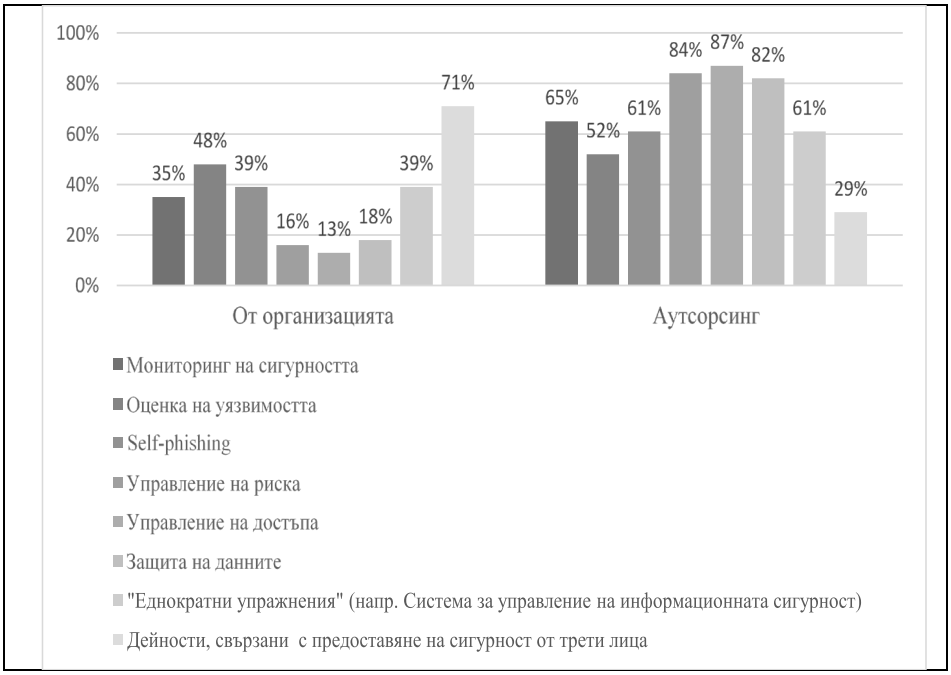
Таблица 2
Топ 10 на най-ценната информация за киберпрестъпниците

Вид информация	**Случаи (процент)**
Информация за клиенти	17%
Финансова информация	12%
Стратегически планове	12%
Информация за членове на Борда	11%
Пароли на клиенти	11%
Информация за изследване и развитие	9%
Информация за сливания и придобивания	8%
Интелектуална собственост	6%
Непатентован IP	5%
Информация за доставчици	5%

Източник: (van Kessel, et al., 2018, p. 9)

Извършителите на неправомерни действия насочват вниманието си към значими зони като **информация за клиенти (17%), финансова информация (12%) и стратегически планове (12%)**. На следващо място са **паролите на клиенти с 11%**, като тази информация е от съществена важност, тъй като тя е предоставена доброволно и клиентите имат доверие на организацията. Това може да окаже сериозен негативен ефект върху репутацията и имиджа ѝ. Не толкова ценна за престъпника е информацията, свързана с доставчиците (5%), непатентования IP адрес (5%) и интелектуалната собственост (6%).

От същото проучване на Ernst & Young са посочени и основните подходи за справяне с киберрисковете (фиг. 2):

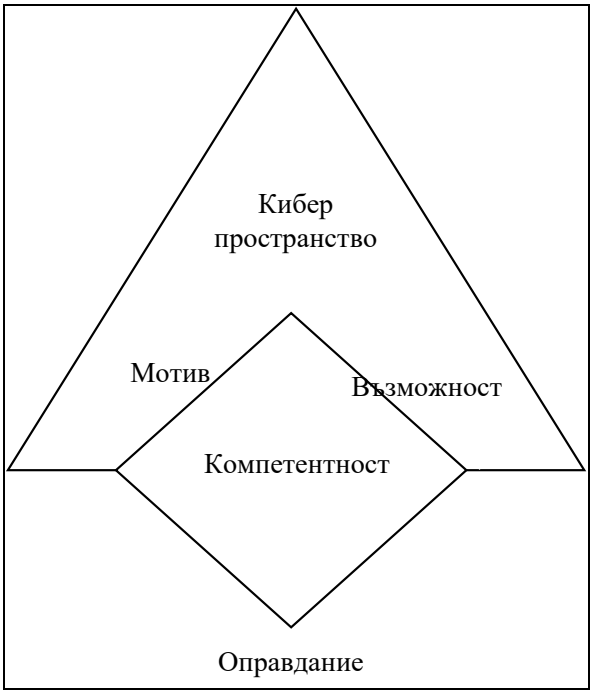


Източник: (van Kessel, et al., 2018, p. 18)

Фигура 2. Подходи, прилагани от организацията и от външни (аутсорсинг) лица

От данните във фигурата се разбира, че основна част от сигурността се осигурява отвън – мониторинг на сигурността (65% аутсорсинг спрямо 35% от организацията), управление на риска (84% аутсорсинг спрямо 16% от организацията), защита на данните (82% аутсорсинг спрямо 18% от организацията). ***Това е сигнал за потенциален риск от кибератаки, тъй като основните дейности, свързани с оценка и поддържане на сигурността, са предоставени на външни лица (компании).***

За да бъдат предотвратени проявните форми на тези заплахи, е необходимо да се проследи по какъв начин елементите на модела „Пентаграм на измамите“ спомагат за това. Този модел е адаптиран от други няколко такива (Триъгълник на измамата“, „Диамант на измамата“, M.I.C.E), с цел предотвратяването и разкриването на измами и оценка на киберриска. Той включва **мотив, възможност за извършване на измама, компетентност, оправдание и кибер пространство**. Към последното се отнасят ***дигитализацията и цифровизацията на процесите, кибертехнологии, разкриване и предотвратяване на киберпрестъпления, оценка на киберриска***. Тази теория може да бъде представена графично по следния начин:



Източник: Разработена от автора

Фигура 3. „Пентаграм на измамите“

Съществен елемент в модела е „киберпространството“, от който произтичат и останалите елементи. Необходимостта от въвеждането му е породена ***от дигитализацията и цифровизацията на процесите, изискванията към съвременните и подходящите знания, умения и компетенции за работа не само с физически (материални) явления и процеси***, ***но и с нематериални (кибер) образи и произтичащите от тях киберрискове.*** В подкрепа на това становище е заключението от Глобалното проучване на икономическата престъпност за 2018 г. (доклад за България) от PwC, в което се посочва, ***че развитието на технологиите предоставя на извършителите нови възможности за атака, но същевременно помага на организациите и одиторите да изградят по-усъвършенствани стратегии за превенция и разкриване*** (Сындби & Мамасян, 2018). Поради това от работата в киберсреда произтичат и останалите елементи, т.е. те са следствие от прилагането на новите технологии в процеса на работа както на одиторите, така и на организациите.

В триъгълника присъстват мотивът и възможността, заедно с компетенциите. Това се дължи на обстоятелството, че **мотивът се свързва с наличието на стимул или действие, които да подтикнат лицето към неправомерни действия. В случая тези действия са следствие от възможностите, които предоставят внедрените технологии – достъп до**

данни, компютърни устройства, финансова информация от разстояние. Възможността **е резултат от неефективен контрол или система, позволяващи на лицето да осъществи противоправно деяние**. Работата в киберпространство благоприятства осъществяването на елемента „възможност“ по различни начини - манипулация на данни, изтриване, промяна, създаване на нови счетоводни или други записи и файлове, прехвърляне на финансова или друга важна за организацията информация, въвеждане на вируси или други зловредни софтуери с цел повреда на персоналния компютър или цялата мрежа.

Показателно за неглижирането на нарастващата заплаха от нов вид и поколение е обстоятелството, ***че 51% от европейските граждани намират, че не са запознати с кибернетичните заплахи, а 69% от фирмите нямат елементарни познания за риска, на който са изложени*** (Съвет на Европейския съюз, 2018). Заедно с това, съвременните системи стават все по-често обект на кибератаки, заразяване с вируси, а борбата с тях и отстраняването им се усложнява. Именно поради тази причина елементът „компетентност“ е от съществена важност, тъй като се свързва с ***нужда от познаване не само на нормативната база, методологията и практиката, но и влиянието на интернет технологиите върху тях.*** Одиторите трябва да притежават определени знания, умения, компетенции за информационните системи, програмните продукти, защото непознаването им може да окаже негативен ефект върху цялостния контролен процес.

Компетентността е позиционирана по такъв начин, явяващ се едновременно като следствие от киберпространството и връзка с последния елемент „оправданието“. Последното е поставено извън фигурата, тъй като е следствие от всички елементи, описани дотук. То предполага, че ***извършителят трябва да формулира някакъв вид морално приемливо оправдание, преди да извърши неморално действие. Оправданието се отнася до това, че неетичното поведение не е неправомерно***. Извършителят приема, че организацията е длъжна да му осигури условията и финансовите средства, които той желае. Като друга връзка, между компетенциите и оправданието, са уменията и знанията, които притежава даденият служител, и недооценеността от работата в организацията. Вследствие на това от служител той става извършител на измама, кражба или друг вид неправомерно деяние.

За вътрешния одит от основно значение е осъществяването на превантивни мерки относно измамите и другите неправомерни действия. Те задължително трябва да оценяват възможността за наличие на измами, а също така и как организацията управлява риска от измами. Вътрешните одитори имат задължението да подпомагат предотвратяването на измами, като проучват и оценяват адекватността на системата за финансово управление и контрол, съответстваща на степента на потенциалния риск в различните сфери от дейността на организацията.

В табл. 3 са ранжирани основните рискове за вътрешния одит:

Таблица 3
Топ 10 на рисковете, стоящи пред вътрешния одит

Рискове за вътрешния одит
Киберсигурност
Информационна сигурност
Проекти за развитие на IT-системите
IT-управление
Външни IT-услуги
Използване на социални медии
Мобилни изчисления
IT-умения сред вътрешните одитори
Развитие на технологиите
Осведомяване на Одитния комитет и Борда за нуждата от технологии

Източник: (Anderson, et al., 2017, pp. 7-3)

Както се вижда от таблицата, **всички рискове са свързани с киберсредата**. Това налага, вниманието на вътрешните одитори и ръководството на организацията да бъде насочено към предотвратяване на тези действия, а за да бъдат редуцирани тези рискове, е необходимо използване на различен инструментариум. Във връзка с потребността от актуализиране на контролите, подпомагащи предотвратяването и разкриването на неправомерни действия, могат да се посочат следните начини, чрез които се спомага за получаване на информация, допринасяща за предприемане на навременни превантивни мерки (Dubis, et al., 2009, p. 21):

- **Кодекс за поведение** – в него се залагат определени дейности, които служителят трябва да извърши през година. Те са свързани с предотвратяването и разкриването на девиантни действия;
- **подаване на сигнал** – това може да стане чрез въведена онлайн платформа или телефон, на който да се съобщават за този вид действия;
- **изходни интервюта** – това са тези разговори, които се провеждат след като лицето е напуснало или е било уволнено. Тези служители могат да дадат информация за съществуващи или предполагаеми схеми, имащи за цел саботиране нормалната дейност на организацията.

Едновременната употреба на превантивни и разкриващи контроли повишава ефективността на всяка Програма за управление на риска. Подходите за разкриване трябва да бъдат приспособими, гъвкави и адекватни на динамичната среда, в която функционира одиторът, т.е. те не са толкова откроряващи се. Докато превантивните са забележими и лесно разпознаваеми.

Разглеждат се и прилаганите организационни подходи на компаниите от т.нар. „Голяма четворка“ (KPMG, PwC, Ernst & Young, Deloitte). Тяхната дейност е насочена предимно към оказване на одиторски, данъчни и рискбазирани услуги, както и различни консултации

– финансови, юридически. Изборът точно на тези одиторски дружества е продиктуван от ресурсите, с които те разполагат (финансови и човешки), и от влиянието, което имат.

Във връзка с това целта на външните одиторите е определяне ***нивото на риск и получаване на разумна степен на сигурност***, че финансовите отчети не съдържат съществени неточности, отклонения и несъответствия, независимо дали се дължат на грешки или измами. В случай че се установят ***неправомерни действия, одиторите съобщават на подходящо управленско ниво***. Поради тази причина оценката, извършена от външните одитори, се възприема за по-безпристрастна и обективна. Независимо от това използваните подходи могат да са много по-иновативни от тези, използвани в одитираната организация или диаметрално противоположното, организацията да разполага с по-високотехнологични такива. Това поражда риск от въвеждане в заблуждение относно извършените операции и сделки. ***Именно затова одиторите, без оглед на тяхната принадлежност, трябва да поддържат своя професионален скептицизъм***.

Често прилаган подход е *оценката на киберготовността (зрелостта) (Cyber Maturity Assessment/CMA), по примера на KPMG*. Тя предоставя възможност да бъде изследвана способността на организацията да защитава активите си, както и готовността ѝ да реагира на кибератаки. *Положителното от прилагането ѝ е, че ръководството получава безпристрастен „поглед“ върху цялостния риск за организацията* (Siriano & Manusakis, 2018, p. 6). Много от вътрешните одитори изпълняват CMA като една от първите стъпки в одита си. Това се дължи на обстоятелството, че тази система предоставя на ръководителите ***оценка за готовността на организацията им да предотвратява, разкрива и да отговаря по подходящия начин на заплахи, свързани с кибератаки.***

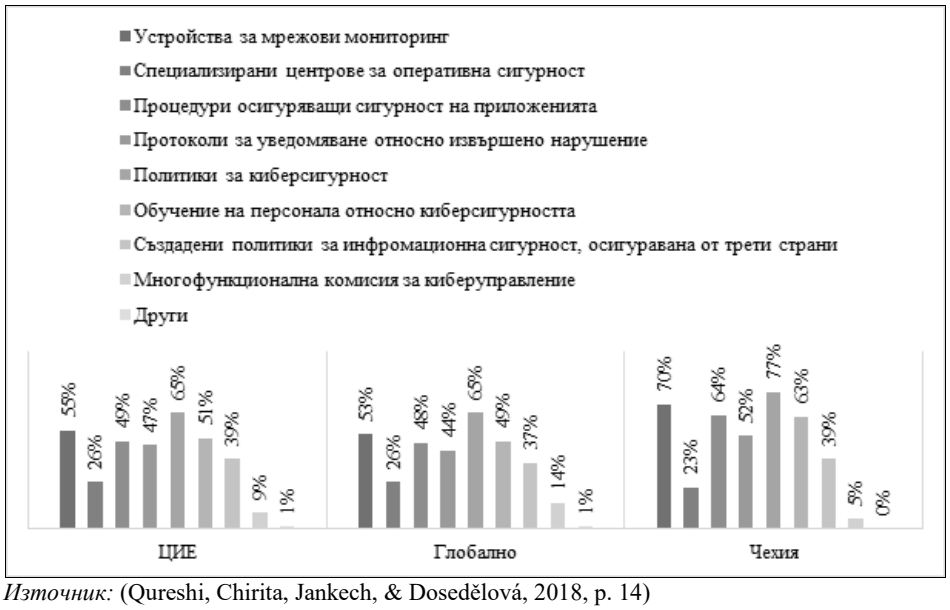
Оценката на киберготовността протича в следните условно приети етапи (KPMG, 2018, p. 1):

1. **Събиране на информация –** придобиване на разбиране за създадената система за сигурност в организацията, възможностите за преодоляване на киберриска, компетенциите на служителите и ръководителите на организацията. В резултат на това могат да се очертаят основните рискове и заплахи за организацията.
2. **Извършване на анализ/оценка –** при осъществяване на определена дейност се проверява риск-регистърът, за да се установи дали и до каква степен тази дейност може да „понесе“ киберриск. По този начин рисковете могат по-лесно да бъдат класифицирани и приоритизирани.
3. **Създаване на стратегия за ограничаване на рисковете –** представят се опции за свеждане на киберриска и риска като цяло до приемливо ниско ниво. Посредством това могат да се установят

проблемните области и да се дадат предложения за ограничаване и предотвратяване на неправомерните действия.

Като част от дадена контролна институция или организация одиторите развиват уменията и компетенциите си, съобразно промените в обекта и настъпилите изменения от технологичен аспект. Все повече субектите на контрол разчитат на технологиите, като например използване на облачни услуги, роботизиране на процесите, което неминуемо води до по-голям риск от кибератаки или извличане на „чувствителна информация“. Във връзка с това PwC **прилага Програма за киберсигурност, която осигурява постоянна информация за заплахите, пред които е изправена организацията, респ. одиторите, сигурност, както и бърза и ефективна ответна реакция** (Qureshi, Chirita, Jankech, & Dosedělová, 2018, p. 13). Посредством нея се гарантира, че одиторите са запознати с тези рискове, както и че поддържат професионален скептицизъм през цялото време.

Значима част от всяка програма е нейното съдържание, т.е. какви елементи са включени в нея. В следващата фигура са представени именно елементите, които са имплементирани в Програмата за киберсигурност (модел на PwC):



Източник: (Qureshi, Chirita, Jankech, & Dosedělová, 2018, p. 14)

Фигура 4. Имплементирани елементи в Програмата за киберсигурност

Данните от фигурата показват, че най-често се използват политиките за киберсигурност както на глобално ниво (65%), така и в страните от Централна и Източна Европа (ЦИЕ) и Чехия, съответно 65% и 77%. ***Това е***

показателно за осъзнатата потребност от този вид политики, с помощта на които е възможно минимализиране на случаите с киберпрестъпления и измами като цяло. Интерес представлява и фактът, че 49% от организациите на глобално ниво осъществят обучения, насочени към киберпрестъпленията и сигурността като цяло. Същото важи и за ЦИЕ с 51% и Чехия с 63%, което е в пъти повече от глобалното ниво. ***Това показва, че грижата за служителите относно тяхната осведоменост и натрупване на определени знания и умения в тази област е от съществена важност.*** Най-рядко използваният елемент е многофункционалният комитет за киберуправление както на глобално ниво (14%), така и на ниво Централна и Източна Европа (9%) и Чехия (5%). В този комитет се включват лица от висшия мениджмънт, маркетолози, финансисти, PR, инженери и други, с председател – главният секретар по информационна сигурност. Тяхната ***цел е да гарантират, че предприятието разполага с подходящи мерки за защита от киберрискове***. Комитетът се отчита за работата си пред Борда на директорите (Jai, 2019), което гарантира за безпристрастността и независимостта на даваните оценки.

Организационният подход, използван от Deloitte, се основава на *Център за киберразузнаване (Cyber Intelligence Center)*. Чрез него се способства за подсигуряване на киберсигурността на всяко ниво в организацията. Той има за цел обединяване и координиране на действия на няколко държави, като се създаде мрежа от професионалисти, с чиято помощ да се гарантира сигурността на клиентите (Wirnsperger & Yildiz, 2017, p. 8). Друг аспект от създаването му е, че сигнали могат да бъдат подавани денонощно на службите, отговарящи за безопасността на личните данни, паролите, финансовата информация. ***Споделянето на данни и информация за настъпили неправомерни действия или бъдещи такива между различните държави, както и между частните и публичните организации, може да подобри в значителна степен управлението на риска***. Например насочване на одиторите и разследващите органи към проблемната област, без предварително да я изследват и оценяват, доставчиците имат функция, с която споделят данни, спомагащи на разследването, като IP адреси, имейл адреси, имена на файлове. След това тази информация се извежда на специални табла за наблюдение на сигурността.

Въз основа на изложението могат да се обобщят следните **изводи:**

Първо. Използването на съвременни технологии в одитния процес поражда нови заплахи и предизвикателства. Последните са ориентирани към онлайн пространството и имат за цел извличане на „чувствителна информация“, като пароли, финансова информация, стратегически планове, информация за клиенти (фишинг, зловреден софтуер). Поради това се налага актуализиране и набавяне на съвременни знания, умения и компетенции. Чрез тях одиторът може да бъде ефективен при установяването на неправомерни действия.

Второ. Оценката на традиционните рискове е недостатъчна за вземане на информирано решение от страна на одиторите относно правилното и навременно отстраняване на слабостите и недостатъците. Поради това вниманието на контролните органи и ръководителите на организациите трябва да се насочи към оценка на нетрадиционните рискове, а именно киберрисковете. Последните възникват в резултат на използване на онлайн средства или системи, чиято цел е получаване на неправомерен достъп до конкретна информация.

Трето. Конвенционалните подходи за справяне с неправомерните действия са неефективни и неадекватни на нововъзникналите и нововъзникващи неправомерни действия. Поражда се нужда от създаването и внедряването на по-иновативни и подходящи подходи, като такива могат да бъдат посочени: „Пентаграм на измамите“, в които се включват дигитализацията и цифровизацията на процесите, кибер технологии, разкриване и предотвратяване на киберпрестъпления, оценка на киберриска; оценка на киберготовността (зрелостта), с помощта на която се преценява доколко съответната организацията е готова да се справи с този риск; Програма за киберсигурност и други.

Заключение

Въз основа на изложеното дотук може да се обобщи, че внедряването и използването на нови технологии е процес, съпътстващ развитието на одиторите и организациите. Същевременно с това обаче тези иновативни технологични системи пораждат заплахи и рискове от нов вид и поколение, целящи извличане на финансова информация, информация за клиенти (вкл. пароли и акаунти), планове за развитие, информация за доставчици, но чрез онлайн средства. Вниманието в одиторската дейност трябва да бъде насочено към опазване на тази „чувствителна информация“ с акцент на киберпространството и киберсигурността. Посредством това се ***съдейства за реализиране на целта на статията***, представяне влиянието на кибер рисковете при технологиите върху одитната дейност и очертаване основните рискове от прилагането им в одита. Последният неизменно трябва да актуализира методическия инструментариум и най-вече подходите, за да може да бъде ефективен, ефикасен и икономичен и да повишава информационната си стойност. Развитието на технологиите подобрява дейността по одит, като предоставя възможност за наблюдение на процесите и дейностите в реално време, набавяне на нужната информация в срок, но заедно с това крие рискове, които имат нова цел и форма – киберпространството. По този начин се постига изпълнението на ***първата задача***, която е свързана с проследяване на влиянието на киберрисковете върху одиторската дейност при работа в киберсреда. Справянето с посочените рискове се постига посредством прилагане на различни организационни

подходи, съдействащи за минимализиране на кибер рисковете – „Пентаграм на измамите“, Оценка на киберготовността (зрелостта), Програма за киберсигурност. В резултат на това се постига втората задача на разработката – извеждане на основните организационни подходи, използвани за минимализиране на кибер рисковете.

Използвани източници

Anderson, U., Head, M., Ramamoorti, S., Riddle, C., Salamasick, M., & Sobel, P. (2017). *Internal Auditing. Assurance & Advisory Services.* Internal Audit Foundating.

Council of Europe. (2001, 09 23). Convention on Cybercrime. Budapest. Retrieved 10 14, 2019, from https://bit.ly/2DDK1TV

Dubis, G., Akresh, A., Jain, P., Morley, L., Phipps, T., & Schmidt, R. (2009). *Internal auditing and fraud.* The Institute of Internal Auditors.

Ellis, A., & Bates, S. (2019). *A changing perspective. Harvey Nash/KPMG CIO Survey 2019.* KPMG.

European Union Agency for Law Enforcement Cooperation. (2018). *Internet organised crime threat assessment.* Europol.

Jai. (2019, 02 26). Enhancing Board Oversight of Cyber Risk. Retrieved 10 16, 2019, from https://bit.ly/2nTk11i

Klimczak, M., Chuprykov, G., & Turczyn, R. (2018). *Global Economic Crime and Fraud Survey 2018: Ukrainian findings. Pulling fraud out of the shadows.* PwC.

KPMG. (2018). Is cyber security top of mind at your business? Retrieved from https://home.kpmg/content/dam/kpmg/ca/pdf/2017/10/cma-slipsheet-kpmg-canada.pdf

Morgan, S. (2019). *2019 Official Annual Cybercrime Report.* Herjavec Group.

Novikova, I., Muller, R., Vostrova, T., Ulyakin, A., & Wood, A. (2018). *Combating fraud: measures taken by companies. Russian Economic Crime and Fraud Survey 2018.* PwC.

Perris, K., & Pikis, M. (2018). *Pulling fraud out of the shadows. 2018 Global Economic Crime and Fraud Survey Highlights. Greece insights.* PwC.

Qureshi, S., Chirita, L., Jankech, P., & Dosedělová, K. (2018). *Global Economic Crime and Fraud Survey 2018. Czech Republic.* PwC.

Siriano, G., & Manusakis, J. (2018). *The role of internal audit in cyber security readiness.* KPMG.

Stoykova, P. (2012). Cybercrime control (cyber control). *First International Conference on Business, Economics and Finance. From Liberalization to Globalization: Challenges in the Changing World* (p. 634). Stip: Univerzitet "Goce Delčev".

Sundbye, P., & Sebov, A. (2018). *Global Economic Crime and Fraud Survey 2018. A front line perspective on fraud in Romania.* PwC.

Tek, C., Major , R., Lim, D., Toh, D., Kosarev, D., Davison, N., Ghosh, K. (2018). *PwC's Global Economic Crime and Fraud Survey 2018 – Singapore Edition.* PwC.

van Kessel, P., Gordon, A., Burg, D., Loughman, B., Watson, R., Vignal, E., Arahari, K. (2018). *Is cybersecurity about more than protection? EY Global Information Security Survey 2018 –19.* Ernst & Young .

Wirnsperger, P., & Yildiz, M. (2017). *A new approach to Cyber Security. Secure. Vigilant. Resilient.* Deloitte.

Инструкцию об организации системы управления рисками в банках, 29 октября 2012 (изменений и дополнений 27 04 2018 г.).

Онищенко, С., & Кирбаба, О. (2017). *Кибер-риски: предстраховая, экспертиза, страхование и урегулирование убытков.* Global cyber security company.

Съвет на Европейския съюз. (11 07 2018 г.). Реформа в областта на киберсигурността в Европа. Изтеглено на 15 10 2019 г. от https://bit.ly/2DMdwo8

Сындби, П., & Мамасян, Р. (2018). *Глобално проучване на икономическата престъпност 2018 г. Доклад за България. Какво остава скрито в сенките?* PwC.

НАУЧНИ ИЗСЛЕДВАНИЯ НА ДОКТОРАНТИ

ГОДИШЕН АЛМАНАХ

Том XII, 2019 г.
Книга 15

СТОПАНСКА АКАДЕМИЯ „Д. А. ЦЕНОВ“ - СВИЩОВ

ГОДИШЕН
АЛМАНАХ
НАУЧНИ ИЗСЛЕДВАНИЯ НА ДОКТОРАНТИ

Том XII, 2019
Книга 15

Академично издателство
„ЦЕНОВ“- Свищов

ISSN 1313-6542

СЪДЪРЖАНИЕ

Студии

Статии

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