УПРАВЛЕНИЕТО НА КИБЕРРИСКА И СЧЕТОВОДНАТА ПРОФЕСИЯ

Михаил Мусов*

Увод

„По заявка номер XXXX ИМА неправомерно разкрити лични данни“ – това е електронното съобщение на Националната агенция за приходите (НАП) за над 2/3 от българските граждани в и над трудоспособна възраст [1]. Тук попадат всички онези лица, чиито лични данни бяха незаконно разпространени в средата на юли 2019 г. при неоторизирания външен достъп до едва 3% от цялата информация в базите данни на НАП. В подобна ситуация – жертва на киберпрестъпление – се оказват над 1 млн. души по света всеки ден (Special Eurobarometer 390, 2012, p. 2). Най-голямото изтичане на данни през 2018 г. беше регистрирано в Индия, където в резултат на серия от кибератаки беше нарушена сигурността на личните данни на всичките 1.1 млрд. жители (WEF, 2019, p. 16). Хакерска атака от септември 2018 г. пък доведе до неправомерен достъп до профилите на 50 млн. потребители на Facebook (Isaac и Frenkel, 2018). Примерите са наистина много – само в САЩ от 2005 г. публично са оповестени над 4 500 случаи на неправомерен достъп до данни (De Groot, 2019), но изводът е един. А той, както алегорично обобщава ръководителят на киберотдела към британска разузнавателна служба MI5, е следният:

> към момента има три сигурни неща в живота – смъртта, данъците и външната разузнавателна намеса във вашата [компютърна] система (Corera, 2013).

В съвременния свят на информационни технологии (ИТ) и свързаност е повече от ясно, че рискът за киберсигурността (за по-кратко – киберрискът) е повсеместен, както и че никоя организация не е защитена. Големите организации имат значително повече ресурси и възможности за инвестиции за повишаване нивото на киберсигурността. Независимо от това, проучване сред над 1 700 изпълнителни директори и мениджъри отговорни за информационната сигурност в някои от най-големите компании в света, устано-

* Михаил Мусов, доктор по икономика, доцент, катедра „Счетоводство и анализ“, УНСС, email: musov@unwe.bg

вява, че 87% от тях нямат увереност в нивото на киберсигурност на техните организации (EY, 2016, p. 7). Малките организации, поради по-ограничените си ресурси, са с относително по-слаби или липсващи контроли за киберсигурност. Това автоматично ги превръща в потенциални жертви на киберпрестъпления. Скорошно проучване разкрива, че при 43% от всички пробиви на бази данни потърпевшите са малки предприятия (Verizon, 2019, p. 5). Обект на кибератаки са както частни, така и публични организации, търговски предприятия и техните глобални вериги за доставка (Моллов, 2016), предприятия от финансовия сектор (Биолчева, 2016), предприятия от сектора на публичните услуги (Йонева, 2018) и неправителствени организации.

Прогнозите сочат, че киберрискът ще продължи да се увеличава, а с това и разходите, които организациите понасят при настъпване на пробиви в сигурността. Основен фактор за това е все по-голямата дигитална свързаност на света, в който живеем. Очакванията са, че през 2020 г. към интернет ще бъдат свързани общо 20 млрд. устройства (Hung, 2017, p. 2). Последното проучване на Световния икономически форум показва, че за предстоящото десетилетие киберрискът се нарежда в топ четири на видовете риск с най-висока вероятност и в топ седем на видовете риск с най-неблагоприятно влияние (WEF, 2019, p. 5). Всичко това превръща правилното разбиране и ефективното управление на киберриска във въпроси от първостепенна важност за всяка една организация.

Целта на настоящата студия е, на база преглед на съществуващата литература, да предложи модел за управление на киберриска и да обоснове ролята на счетоводната професия в нея. Основната теза на автора е, че за ефективното управление на киберриска е необходим модел, който балансира ограничаването на неблагоприятните последици и използването на благоприятните възможности за развитие, предоставени от съвременната киберсреда – модел, който предоставя много възможности за развитие пред счетоводната професия, но тяхното използване зависи от адекватна промяна във висшето образование по счетоводство. В първата част е дефинирана същността на киберриска. Въз основа на изведената дефиниция във втората част киберрискът е разгледан като триединство на опасност, ИТ уязвимост и неблагоприятни последици от нарушаването на киберсигурността в организацията. В третата част е предложен авторов модел за ефективно управление на киберриска. В последната част са разгледани компетенциите, необходими на бъдещите професионалисти за целите на ефективното управление на киберриска, и са дискутирани възможностите на висшето счетоводно образование да допринесе за развитието на тези компетенции. Изводите са подобаващо обобщени в заключението.

Изследването се базира на проучване на съществуващата литература. Широко се прилагат методите на анализа и синтеза, методът на моделирането, системният подход и други методи на научното познание. Използваният дедуктивен подход обосновава широката приложимост на крайните изводи.

Същност на киберриска

Макар киберрискът да е пряко свързан с ИТ инфраструктурата (в т.ч. софтуер и хардуер), погрешно би било да се възприема единствено и само като технически проблем, който трябва да бъде решаван от ИТ специалистите. Управлението на киберриска следва да се разглежда в контекста на цялостното управление на риска на предприятието (от англ. – enterprise risk management). От тази гледна точка към техническото измерение на киберрискът се прибавят и неговото организационно и поведенческо естество (IRM, 2014, p. 10).

Съществуващите в литературата определения за киберриска не се различават съществено помежду си. Всъщност, ето и някои от тях:

1. Институтът за управление на риска (Institute of Risk Management – IRM) разглежда киберриска като

> всеки риск от финансови загуби, срив или увреждане на репутацията на организацията в резултат на неправилно функциониране на нейните ИТ системи (IRM 2014, p. 10).

Според Института киберрискът може да се реализира по следните три начина: (а) чрез умишлено и неоторизирано нарушаване на сигурността с цел достъп до информационните системи; (б) чрез непреднамерено нарушаване на сигурността и (в) в резултат на лош интегритет на системите или други фактори.

2. Женевската асоциация (Geneva Association), в която членуват някои от най-големите застрахователни и презастрахователни компании в света, определя, че киберрискът е

> всеки риск, възникващ от използването на информационни и комуникационни технологии (ИКТ), който компрометира конфиденциалността, достъпността и целостта на данни или услуги (GA, 2016).

В това определение се включва както рискът, който може да възникне в резултат на самите технологии, така и този, който е резултат от човешка намеса.

3. Британският Национален център за киберсигурност (National Cyber Security Centre – NCSC) приема киберриска като

> потенциала на една заплаха (лице или предмет, които са вероятни причинители на щета) да използва уязвимост (недостатък, функционална особеност или грешка на потребителя), която може да доведе до някаква форма на отрицателно въздействие (NCSC, 2016, p. 4).

В основата на това разбиране за киберриска е уязвимостта, която предоставя възможността дадени заплахи да се превърнат в негативни последици. Тя може да възникне в резултат на недостатък на системата (непредвидена функционалност вследствие на лошо проектиране или грешки при внедряването), функционална особеност на системата (предвидена функционалност, която при злоупотреба да доведе до нарушаване на сигурността) и грешки на потребителите на системата.

Краткият обзор на преобладаващите в литературата становища позволява формулирането на следната дефиниция: киберрискът е *потенциалната опасност* една *уязвимост*, възникнала при използването на ИТ инфраструктурата, да доведе до *неблагоприятни последици* за дадена организация и/или свързани с нея заинтересовани страни. От така представеното определение се разбира, че:

- потенциалната опасност е опасност с определена степен на вероятност, която може да е съществуваща или да възникне в бъдеще;
- ИТ уязвимостта може да има за източник самите ИТ системи или пък да е резултат от грешка на потребителите;
- последиците от нарушаването на киберсигурността могат да имат неблагоприятно въздействие върху самата организация и/или върху нейните клиенти, доставчици и други заинтересовани страни.

В следващата част на студията това триединство (вж. фигура 1) е използвано като основа за по-подробна дискусия на отделните аспекти на киберриска.

Фиг. 1. Същност на киберриска

Триединството на киберриска – опасност, ИТ уязвимост и неблагоприятни последици

Опасността може да идва отвън или отвътре и да е предизвикана от различни мотиви

Извършителите. Потенциалната опасност от нарушаване на киберсигурността може да има *различни източници*. Съгласно доклада на Verizon (2019) участниците в разкриването на данни могат да бъдат отнесени в три основни категории:

- външни лица – тук попадат лица от организираната престъпност, бивши служители, познати лица, конкуренти, клиенти и др. Те са отговорни за около 70% от случаите на изтичане на данни;
- вътрешни лица – включват системни администратори, крайни потребители на данни в организацията и други лица от различните отдели. Отговорни са за около 30% от инцидентите с изтекли данни;
- партньори – отговорни са за до 5% от киберинцидентите.

Мотивите. Лицата, които нарушават киберсигурността, са водени от *различни мотиви*. В преобладаващата част от случаите (над 75% за 2018 г.) мотивът е финансов (Verizon, 2019). Такъв е мотивът на различни форми на киберпрестъпления: заплахи, изнудване, атаки спрямо мрежи и системи с цел преустановяване на услуги и др. В немалък брой от случаите (около 25% за 2018 г.) целта е шпионаж с цел получаване на стратегическо предимство. Обект на интерес представлява информация за предстоящи сливания и придобивания на компании, намерения за съвместни предприятия, насоки за стратегическо развитие и др. Нерядко този шпионаж се извършва от чужди държави. В ограничен брой от случаите мотивът е доказване на професионални умения от страна на т.нар. киберактивисти (от англ. – activists) – лица с опортюнистично поведение, чиято цел е просто да причинят смущения в ИТ системите или да демонстрират своите ИТ умения.

Средствата. Проучванията сочат, че киберпрестъпниците преобладаващо използват следните два основни инструмента (AICPA, 2019):

- *зловреден софтуер* (от англ. – malware), който най-често е: вирус (от англ. – virus) – софтуер, който разрушава компютърната система или унищожава данни; червей (от англ. – worms) – софтуер, който може да контролира компютърната мрежа без знанието на основния оператор; рансъмуер (от англ. – ransomware) – софтуер, който ограничава достъпа до файлове с цел заплащане на откуп от потребителя или
- различни *хакерски техники* с цел кражба на данни за целите на извършването на последващи измами.

ИТ уязвимостта е резултат от използваната и/или от използването на ИТ инфраструктура

ИТ инфраструктурата може и да е основният източник на уязвимост, която предоставя възможността потенциалните опасности да се превърнат в негативни последици, но не е единственият. Другият източник на уязвимост са потребителите на ИТ системите – служителите на организацията. Larry Ponemon, председател и основател на Института Понемон (Ponemon Institute) – изследователския център за защита на данните и киберсигурността, формулира тезата по следния начин:

> Повечето хора гледат на хакера като на лошия човек в трилър филм, който прониква [в системата] и предизвиква хаос, но далеч преди него най-големият риск за една организация е вътрешният проблем… Понякога това е злонамерен вътрешен човек, а понякога е добър човек, който върши глупави неща (Adamek, 2019).

В много случаи служителите неволно съдействат на външните извършители, с което значително улесняват пробива на киберсигурността на организацията. Изследванията сочат, че неволни грешки на служителите са причина за 21% от случаите на изтичане на данни през 2018 г. (Verizon, 2019). Казано по друг начин, ако не бяха грешките на потребителите, един от всеки пет случая на пробив на информационната сигурност нямаше да съществува. Следователно, *служителите* следва да бъдат във фокуса на всяка една ефективна стратегия за управление на киберриска – от етапа на оценка на киберриска през обучението и мониторинга, до създаването на организационна култура на осъзнаване на риска и отговорно отношение към сигурността на информацията.

Неблагоприятните последици са големи и рядко засягат единствено организацията

Неблагоприятните последици от нарушаването на киберсигурността могат да бъдат наистина многоаспектни – в планетарен мащаб те имат потенциала да причинят „големи икономически щети, геополитическо напрежение и широко разпространена загуба на доверие в интернет“ (WEF, 2019, p. 98). Обикновено разходите в резултат на нарушаване на киберсигурността се класифицират в две групи: разходи, които не подлежат на застраховане, и разходи, които подлежат на застраховане.

Разходи, които не подлежат на застраховане. В тази група на разходите се отнасят (IRM, 2014, pp. 31–37):

- глоби, свързани с нарушаване сигурността на информацията – налагат се в зависимост от съществуващото законодателство в държавата, в която се извършва дейността [2];

- увреждане на репутацията – неблагоприятно влияние върху репутацията на организацията или нейни брандове;
- загуба на клиенти – свързана е с непосредствената загуба на клиенти, отлива на бъдещи клиенти и евентуалната невъзможност за участие в обществени поръчки;
- загуба на служители – свързана е с напускането на служители, които не желаят да бъдат част от организация, претърпяла киберинцидент;
- обезценяване на акциите – негативният отзвук в резултат на киберинциденти често води до намаляване цената на акциите;
- обезценяване на интелектуална собственост на организацията – евентуална кражба на интелектуална собственост може да доведе до нейното пълно обезценяване, а в някои случаи и до ликвидирането на организацията;
- преки разходи, които трябва да бъдат извършени във връзка с предприемането на корективни мерки, в т.ч. разходи за подобряване на ИТ инфраструктурата.

Разходи, които подлежат на застраховане. Част от киберриска и разходите, асоциирани с него, могат да бъдат прехвърлени на застрахователни компании. В тази група на разходите се включват (IRM, 2014, pp. 209–219):

- разходи за експертизи за определяне на обхвата на киберинциденти;
- разходи за уведомяване на трети страни;
- разходи за издръжка на колцентър с цел предоставяне на допълнителна информация на засегнатите страни;
- разходи за услуги по предотвратяване на измами (например, с разкрити лични данни на клиенти);
- разходи за PR услуги по ограничаване на вредите върху репутацията на организацията;
- разходи за правно обслужване и съдебни искове;
- пропуснати приходи;
- разходи за възстановяване на нематериални активи (например, бази данни, клиентски листи, спецификации и др.);
- разходи, свързани с киберизнудвания, и др.

Независимо че всички тези разходи могат да бъдат част от застрахователните полици, много от организациите не разчитат единствено на прехвърлянето на риска, а на неговото активно управление. Това е така, защото понесените щети в повечето случаи надхвърлят застрахователните обезщетения.

Предложен модел за ефективно управление на киберриска

Традиционното разбиране е че всеки процес на управление на риска, в т.ч. и управлението на киберриска, има за цел да минимизира вероятността за и последиците от неблагоприятни събития. Такава е и дефиницията, предложена от Асоциацията на международните сертифицирани професионални счетоводители (Association of International Certified Professional Accountants – AICPA), според която управлението на киберриска е:

> съвкупността от действия, които могат да бъдат предприети за идентифициране, оценка, смекчаване, превенция, избягване, застраховане, както и за мониторинг и мениджмънт на или подготовка за рисксъбития – или за ограничаване на щетите след събитие (AICPA, 2019).

Това разбиране обаче е непълно, тъй като се фокусира единствено върху минимизирането на щетите и не взема под внимание множеството бизнес възможности за развитие, които новите технологии предлагат. Примери за такива могат да бъдат: навлизането на интернет на нещата (от англ. – internet of things), използването на големи бази данни (от англ. – big data), употребата на лични устройства на служителите за служебни цели и др. Оползотворяването на тези възможности с цел повишаване на ефикасността на дейността и достъп до нови пазари и клиенти поначало предполага използването на повече нови технологии, на по-голяма свързаност и т.н., което, при равни други условия, излага организацията на по-високи нива на киберриск. Оттук, ако единствената цел е минимизиране на неблагоприятните последици, това може да доведе до отхвърляне на нови възможности. Обратното също вярно:

> прекалено силният фокус върху възможностите води до това предприятието да бъде изложено на ниво на риск, превишаващо допустимия толеранс; прилагането на твърде строги контроли за управление на информационния риск ограничава способността за успешно оползотворяване на възможностите (IRM, 2014, p. 69).

Следователно, правилното разбиране на управлението на киберриска е свързано с постигането на ефективен *баланс* между ограничаването на неблагоприятните последици и използването на благоприятните възможности за развитие, които съвременната киберсреда предпоставя. Именно към този баланс следва да бъдат насочени всички усилия по управлението на киберриска в организациите.

В специализираната литература съществуват различни модели за управление на киберриска. Три от най-новите и широко използвани в прак-

тиката модели са представени в приложение, както следва: *Приложение 1* – модел на National Cyber Security Centre към британското правителство (NCSC, 2012); *Приложение 2* – модел на Association of International Certified Professional Accountants (AICPA, 2019); *Приложение 3* – модел на Eaton, Grenier и Layman (2019). Възможно е да се изследват и представят още модели за управление на киберриска, но общият извод няма да се промени. А той е, че ефективното управление на киберриска изисква използването на холистичен подход. Без него, управлението на киберриска ще бъде просто съвкупност от зле координирани и половинчати политики и дейности, които в най-добрия случай биха имали посредствен резултат.

По-долу, представените в приложение модели са интегрирани и допълнени с цел разработването на *модел за ефективно управление на киберриска*, в който да се идентифицира мястото на счетоводната професия. Предложеният модел разглежда управлението на киберриска като динамично проявление на шест взаимосвързани етапа (вж. фигура 2), които са последователно представени по-долу.

Фиг. 2. Модел за ефективно управление на киберриска

ЕТАП 1. Идентифициране, приоритизиране и оценка на киберриска

Процесът на управление на киберриска започва с неговото идентифициране, приоритизиране и оценка. Това е основата за предприемането на най-ефективните стратегии за управление на киберриска (избягване на риска; намаляване на вероятността и на неблагоприятните последици; пълно или частично прехвърляне на трети страни; задържане на риска с цел оползотворяване на възможностите), както и за тяхното адекватно ресурсно обезпечаване.

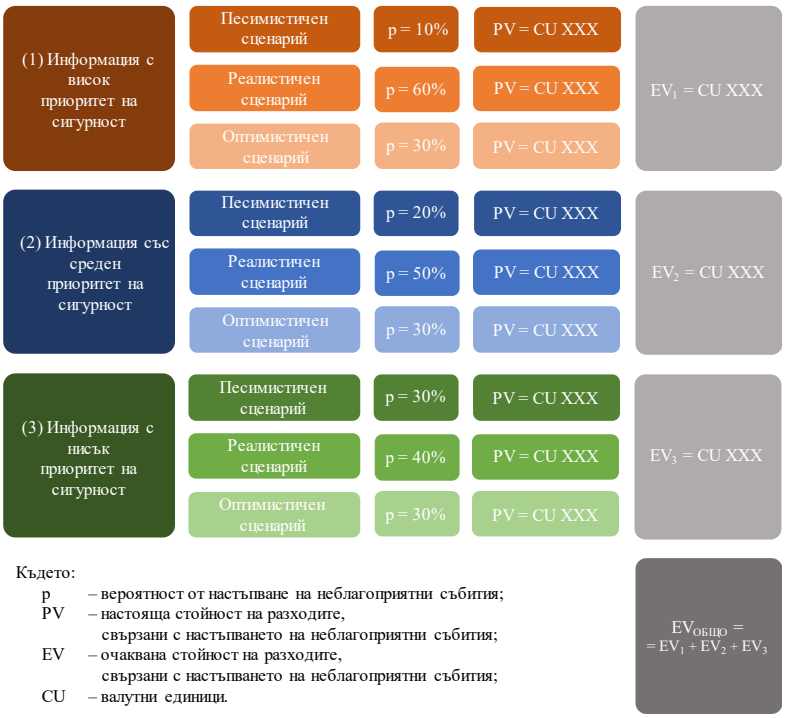
Идентифицирането и *приоритизирането* касаят както потенциалните заплахи и източниците на уязвимост, така и чувствителността на информацията, съхранявана в ИТ системата. Организациите разполагат с различна информация – клиентски данни, данни за кредитни карти, интелектуална собственост, финансови данни, данни, свързани с бизнес стратегията и др. Различната информация е с различна степен на важност (ценност) за организацията. Оттук, логично е да се приеме, че прилагането на една единствена стратегия за управление на риска спрямо цялата налична информация е неоправдано – в едни случаи това би означавало излишни разходи, а в други – недостатъчна защита на информацията. Въпросът следователно е за подхода на диференциране. Рационално решение е организацията да приоритизира информацията в категории според степента на важност – например, с *висок*, *среден* и *нисък* приоритет. Спрямо отделните категории е възможно да се следват различни стратегии за управление на риска. Например, за информацията с висок приоритет организационният мениджмънт може да приложи стратегия на елиминиране на риска; за информацията със среден приоритет – стратегия на намаляване или прехвърляне на риска; за информацията с нисък приоритет – стратегия на намаляване, прехвърляне или задържане на риска.

Оценката на експозицията на киберриск е не по-малко важна за неговото ефективно управление. За да е полезна, тази оценка следва да бъде *уместна* и *надеждна*. Две са съображенията в тази насока. Първо, паричните оценки са по-уместни от качествените. Качествени оценки от вида на „нисък“ или „висок“ риск се считат за недостатъчно полезни, тъй като „не помагат на мениджърите да разберат дали имат проблем в размер на 10 млн. долара или такъв в размер на 100 млн. долара“ (Chacko, Sekeris и Herbolzheimer, 2016). Второ, за да е надеждна, парична оценка на киберриска трябва да взема под внимание всички разходи, свързани с възникването на потенциално неблагоприятно събитие – преките разходи, свързани с настъпването на събитието; пропуснатите приходи и разходите в резултат, възникващи в резултат увреждане на репутацията. В общия случай паричната оценка ще бъде настоящата стойност на всички тези елементи на разходите.

Важно е да се отбележи, че приоритизирането на информацията в различни категории според степента на важност има положително влияние както върху уместността, така и върху надеждността на оценката на киберриска. От една страна, приоритизирането на информацията позволява изготвянето на отделни парични оценки на киберриска за всяка от идентифицираните категории информация. Всяка една оценка е индикатор за максималната стойност на разходите, които организацията може да си позволи да извърши за целите на управлението на киберриска за съответната категория информация. Например, възможно е паричната оценка на киберриска за информацията с висок приоритет да възлиза на милиони, докато оценката на киберриска за информацията с нисък приоритет да бъде многократно по-ниска. Съобразяването на мерките за управление на киберриска с отделните оценки е по-уместно отколкото базирането им на една единствена агрегатна оценка на общата рискова експозиция на организацията, защото води до по-оптимално разпределение на разходите, а с това и до повишаване на тяхната ефикасност.

От друга страна, приоритизирането на информацията е предпоставка и за по-надеждното оценяване на киберриска. Известно е, че рискът е неизменно свързан с вероятностите за настъпването на потенциални неблагоприятни събития. Оценките на тези вероятности (т.нар. вероятности разпределения) са в основата на оценяването на риска. За различните категории информация обаче вероятностните разпределения могат да бъдат различни. Например, рискът от цялостна загуба на информацията с висок приоритет може да бъде едва 10%, докато този от загуба на информацията с нисък приоритет – 50%. Оттук, приоритизирането на информацията позволява използването на множество вероятности разпределения, които от своя страна водят до по-надеждна парична оценка на киберриска както за отделните категории информация, така и общо за организацията.

Фигура 3 цялостно илюстрира първия етап от управлението на риска. Първоначално идентифицираната чувствителна информация се приоритизира според степента на важност (например, с висок, среден и нисък приоритет). За всяка от категориите информация се разглеждат различни сценарии (например, песимистичен, реалистичен и оптимистичен). За всеки отделен сценарий се определя вероятност от настъпване (p) и се изчислява настоящата стойност (PV) на разходите, свързани с възникването на потенциални неблагоприятни събития. Въз основа на това за всяка категория информация може да бъде изчислена очакваната стойност (EV) на разходите при настъпване на неблагоприятни събития [3]. В зависимост от получените оценки и индивидуалната склонност към риск, организационният мениджмънт следва да избере стратегии за управление на риска и да предприеме необходимите действия по тяхното реализиране.



Фиг. 3. Идентифициране, приоритизиране и оценка на киберриска

ЕТАП 2. Въвеждане на система за контрол на киберриска

Вторият етап е свързан с въвеждането на контроли с цел ефективното управление на киберриска. Тези контроли трябва да осигуряват спазване на външните регулации и да са в съответствие с вътрешните политики и цялостното управление на риска в предприятието. Възможно е да бъдат разработени:

- контроли за управление на привилегировани потребителски акаунти;
- контроли за сигурността на конфигурацията на цялата система и на мрежата, включително за защита от зловреден софтуер;
- политика за работа извън офиса;
- политика за контрол на достъпа до преносимите носители на информация и др.

В съвременния дигитален свят, в който организациите са свързани една с друга, управлението на киберриска единствено в рамките на предприятието не е достатъчно. За да бъдат данните защитени, контролите и политиките трябва да бъдат въведени във всички организации от веригата за доставка.

Обучението и информираността на потребителите са важни за привеждането на системата за контрол на киберриска в действие както в самата организация, така и в организациите от веригата за доставка [4]. Погрешно е обаче да се приема, че те имат първенстващо значение, както и че превъзхождат останалите елементи. Това е така, защото управлението на риска е холистичен процес, който не може да бъде сведен единствено и само до обучение и информираност. Професионалисти по киберсигурност правилно отбелязват, че

> сега съществува цяла индустрия, която обучава нас, хората, да сме по-интелигентни в работата с компютрите и въпреки това броят на инцидентите с киберсигурността продължава да нараства. Винаги ли хакерите са с една стъпка напред? Невъзможно ли е да бъдем обучени? Или ни преподават погрешни уроци? … Просто има толкова много шансове случайно да повредим … мрежите, с които работим, независимо от това колко сме обучени (Sulmeyer и Dugas, 2017).

От казаното може да се заключи, че известно обучение по киберсигурност е полезно, тъй като има потенциала да доведе до намаляване на киберриска до определено ниво, но по-нататъшното намаляване или елиминиране на риска не може да бъде постигнато с допълнително обучение. По-нататъшното намаляване на нивото на риска изисква мерки, различни от обучение – например, инвестиции в нови ИТ системи, преминаване към облачни услуги и др.

Управление на киберриска в облачна среда. Използването на облачни услуги – аутсорсването на ИТ функции към външен доставчик – става все по-разпространено. През 2018 г. 26% от всички предприятия в ЕС използват такива услуги (Eurostat, 2018). Като цяло използването на облачни услуги не се счита за източник на допълнителен киберриск. Детайлно сравнение между средата с използване на традиционна ИТ инфраструктура и облачната среда, извършено от Института по управление на риска, разкрива следния общ извод:

> облакът нито увеличава, нито намалява профила на риска; ефективно контролираната среда, прехвърлена към облака, ще продължи да бъде ефективно контролирана, ако контролите останат на място, докато лошо контролираната среда ще остане изпълнена с риск и заплахи, независимо от избора на ИТ инфраструктура (IRM, 2014, p. 102).

Традиционно се препоръчва внимателен избор на доставчика на облачни услуги и включване в договора на клаузи, осигуряващи адекватна защита на организацията в случай на нарушаване на киберсигурността.

Управление на киберриска при използването на мобилни устройства (различни от компютрите). Използването за служебни цели на мобилни устройства носи ползи за организациите – по-ниски разходи и по-висока производителност на труда, но също така и допълнителен киберриск. Политиката на отделните организации варира от безконтролното използване на лични мобилни устройства през използването единствено на служебни такива, до тяхната пълна забрана. Относно управлението на киберриска при използването на мобилни устройства се препоръчва да се търси „баланс между това, което потребителите желаят, и това, от което организацията се нуждае“ (IRM, 2014, p. 132). Като цяло е необходимо регламентиране на начина, по който мобилните устройства могат да бъда използвани в организацията, на отделни елементи на тяхната конфигурация (например, минимални изисквания към сигурността на паролите), на отговорността за сигурността на данните, които са достъпни през мобилното устройство, и др.

Управление на киберриска при използването на социални медии. Използването на социалните медии от организациите непрекъснато се увеличава – през 2017 г. 47% от предприятията в ЕС използват поне една социална медия, докато през 2013 г. този процент е бил едва 28% (Eurostat, 2017). Организациите използват социалните медии за различни цели – маркетинг на продукти, бърза комуникация със заинтересованите страни, набиране на кандидати за работа и др. Малко от тях обаче осъзнават, че социалните мрежи увеличават нивото на киберриска в организацията. Допълнителният риск може да е свързан с ползвателите на социалните мрежи и/или технологиите и/или споделяната информация (IRM, 2014, pp. 144–150). Мерките за управление на този тип киберриск отново касаят разработването на правила за използване на социалните медии, обучение на персонала, мониторинг на страниците на организацията в социалните мрежи, отношение с грижа към негативните коментари или оплакванията на клиенти и др.

ЕТАП 3. Мониторинг на системата за контрол на киберриска

Третият етап е свързан с непрекъснат мониторинг на разработените и въведени политики и контроли с цел незабавно разкриване на инциденти с киберсигурността. Добра практика е да бъде разработена стратегия за мониторинг.

Като част от оценката на ефективността на системата за контрол на киберриска може да се провежда и регулярен вътрешен одит. По дефиниция вътрешният одит представлява:

> независима, обективна дейност по осигуряване на сигурност и консултиране, предназначена да добавя стойност и да подобрява дейността на организацията. (IIA, 2019).

Възможно е вътрешните одитори да фокусират вниманието си върху три вида контроли: (IRM, 2014, 245–246):

- превантивни – контроли, предназначени да предотвратяват настъпването на дадено събитие (например, решения за превенция на загубата на данни; решения за защита от зловреден софтуер и др.);
- разкриващи – контроли, предназначени за ранно предупреждение (например, мониторинг на ИТ системите);
- коригиращи – контроли, предназначени да коригират щетите при настъпили вече събития (например, наличие на план за продължаване на дейността).

ЕТАП 4. Управление на инциденти с киберсигурността

Тъй като киберрискът никога не може да бъде напълно елиминиран и винаги съществува вероятност от настъпване на инцидент с информационната сигурност, управлението на инцидентите е неотменима част от цялостния процес на управление на киберриска. Управлението на киберинциденти има множество цели, основните сред които са: разкриването и оценката на инцидента; минимизирането на щетите; идентифицирането на причините и предприемането на мерки за подобряване.

В съответствие с тези цели са и петте ключови стъпки на процеса (IRM, 2014, pp. 181–187):

- подготовка – разработване и тестване на правила за действие в случай на инцидент; определяне на екип от отговорни лица, които да поемат изпълнението на останалите четири етап в процеса;
- разкриване и оценка – оценка на влиянието на инцидента върху информационната система;
- отговор и задържане – бързо и ефикасно от гледна точка на разходите предупреждаване на потенциалните жертви и ограничаване на по-нататъшната загуба на данни;
- възстановяване – възстановяване на оперативната способност на системите и процесите и предприемане на действия за предотвратяване на повторно възникване на инцидента;
- подобряване – преглед и оценка на предприетите действия по предходните четири етапа, включително изготвяне на доклад за инцидента.

ЕТАП 5. Отчитане на управлението на киберриска и независим одит

Петият етап касае отчитането на управлението на киберриска пред външни заинтересовани страни и провеждането на независим одит. Целта на отчитането е да се предостави информация относно наличните системи, политики и мерки по управление на киберриска, както и относно това дали контролите са функционирали ефективно през отчетния период. Целта на независимия одит на отчитането е да се повиши увереността на външните потребители в изготвения отчет за управлението на киберриска.

Този етап не е задължителен за организациите, но е свързан с редица ползи. Според едно скорошно проучване оповестяването на политиката по управление на риска носи информация на инвеститорите и може да допринесе за смекчаване на негативното въздействие при евентуален неправомерен достъп (Eaton, Grenier и Layman, 2019). Друго изследване също сочи, че клиентите очакват прозрачност от компаниите по отношение използването и защитата на техните лични данни (Deloitte, 2018), а отчитането и одитът са най-добрите начини за нейното осигуряване.

ЕТАП 6. Неформално (скрито) управление на киберриска

Неформалното (или скрито) управление, в чиято основа е организационната култура, традиционно не се разглежда като самостоятелен етап в процеса на управление на киберриска. Не липсват обаче публикации (IRM, 2014, 48; Hogg 2017), които признават неговата роля при формирането на капацитет за справяне с киберзаплахите. Няма да е погрешно, ако скритото управление на киберриска се представи като съвкупност от всички онези неформални и понякога непреднамерени ценности, вярвания и нагласи, които, наред с формалното управление на организацията, определят отношението на служителите към сигурността на ИТ системите и информацията. Например, иновативните и небюрократични организации се характеризират с по-бърз информационен поток и като такива, при равни други условия, биха били по ефективни при управлението на киберриска, отколкото организациите със силно изразена бюрократична структура. По подобен начин, организациите, в които ефективността се оценява на базата на съвкупност от финансови и нефинансови показатели, също биха били по-добри в управлението на киберриска, тъй като при равни други условия, биха били склонни да извършват по-големи инвестиции за повишаване нивото на киберсигурност, отколкото организациите, в които оценката се базира единствено или приоритетно на финансови показатели.

Разкриването и използването на пълния потенциал на скритото управление на риска изисква много допълнителна и упорита изследователска рабо-

та. Дотогава обаче академичните и професионалните среди следва да имат предвид неговата всепроникваща сила.

Счетоводната професия и управлението на киберриска

Компетенциите, необходими на бъдещите професионалисти по киберсигурност, са преди всичко базови (личностни), а не технически

Пазарът на продукти и услуги в областта на киберсигурността непрекъснато се увеличава. Той се оценява приблизително на 1 трилион долара за периода 2017 – 2021 г. (Morgan, 2019). Същевременно, прогнозите сочат, че до три години в света ще има над 1.8 млн. свободни работни места за специалисти в областта на киберсигурността (Reed, Zhong, Terwoerds и Brocaglia, 2017, p. 7). На фона на тези очаквания все по-отчетливо ясно става, че въпросната пазарна ниша не може да бъде запълнена с формално университетско образование:

> Работодателите са все по-притеснени за релевантността на образователните програми, свързани с киберсигурността, спрямо нуждите на техните организации (The U.S. Secretary of Commerce and the U.S. Secretary of Homeland Security, 2018).

Организациите намират решението в компетентностния подход – набират професионалисти от всички области на познанието, стига да считат, че компетенциите им могат да осигурят сигурност на информацията.

Логичният въпрос е, какви са компетенциите, които бъдещите професионалисти по киберсигурност трябва да притежават. Отговор дава изследване на IBM Института за бизнес стойност, според което необходимите компетенции могат да бъдат отнесени в две групи (вж. Таблица 1): основни качества (от англ. – core attributes) и умения (от англ. – skills):

> Основните качества могат да се приемат като общи качества, присъщи на човека, които са от полза за специалистите по сигурността – съвкупност от общи черти на личността и поведение, придобито в резултат на учене. Уменията включват както технически способности, така и способности, свързани с работното място (IBM Institute for Business Value, 2017, p. 6).

Важно е да се подчертае, че от професионалистите по киберсигурност не се изисква да разполагат с всички тези качества и умения в началото на своето кариерно развитие. Задължително е обаче те да имат нагласата да ги развиват във времето. Приема се, че това „ще осигури по голяма гъвкавост

в развитието на кариерата, както и основата за заемане на … ръководни позиции“ (IBM Institute for Business Value, 2017, p. 6).

Дори и бегъл поглед на предложените в Таблица 1 умения е достатъчен, за да се установи, че почти всички от тях спадат към групата на базовите (личностни) умения (от англ. – soft skills). Тук се включват например: аналитичните умения, уменията за решаване на проблеми, желанието за непрекъснато учене, етичното поведение, комуникационните умения и т.н. Техническите умения са силно ограничени – строго погледнато, сведени са единствено до „познания и известни способности в програмирането“. Това не би трябвало да изненадва никого в професионалните среди. Скорошно проучване, проведено сред 315 професионалисти по киберсигурност, работещи в организации с над 100 служители, показва, че всички (100% от респондентите) считат базовите (личностните) умения за важни, а всеки пети от запитаните дори намира тези умения за *по-важни* от техническите (Lapena, 2017). Вероятно това е и причината, поради която 17% от запитаните очакват в бъдеще да наемат служители за целите на управлението на киберриска, които нямат експертиза в областта на киберсигурността (Lapena, 2017).

Таблица 1. Основни качества и умения на професионалистите по киберсигурност

Основни качества		Умения
Анализиращ	Изследователски настроен и обичащ предизвикателствата	Вродено разбиране за риска, възможните сценарии и „what ifs“ анализите
Решаващ проблеми	Аналитичен, методичен и ориентиран към детайла	Практически опит
		Познания и известни способности в програмирането
Желаещ да учи	Учещ непрекъснато	Знание специфично за отрасъла
		Способност за адаптиране към нови и възникващи технологии
Защитаващ	Етичен и надежден	Познаване на приложимата нормативна уредба и способност за нейното интерпретиране
Сътрудничещ	Способен да работи с други лица	Способност за работа в динамичен екип от различни хора
		Умения за ефективна комуникация – изразяване на сложни концепции и ясно обясняване на технически проблеми
		Опит в обучаването на други

Източник: Базирано на IBM Institute for Business Value (2017, p. 7).

Ролята на счетоводната професия в управлението на киберриска на организацията може да бъде всестранна

Понастоящем академичните среди, професионалните организации на счетоводители и одитори, както и големите одиторски компании са единодушни, че счетоводната професия може и трябва да има водеща роля в управлението на киберриска. По-долу последователно са представени позициите и на трите страни.

Позицията на академичните среди. Една от последните статии, публикувани в издание на Американската счетоводна асоциация, е посветена на разкриване ролята на професионалните счетоводители във всеки един от етапите на управлението на киберриска (вж. Eaton, Grenier и Layman, 2019). Според авторите на статията това, което създава предимство на счетоводните и одиторските предприятия пред останалите организации, е специфичното знание в областта на вътрешния контрол, финансовото отчитане и независимия финансов одит. На етапа на идентифициране и приоритизиране на риска те считат, че консултантските отдели на големите одиторски компании могат да бъдат полезни не само с това, че са наясно с новите и възникващи заплахи, но и със своя опит в оценяването на вероятността и обхвата на различни заплахи. На следващите етапи – при проектирането и тестването на ефективните контроли на киберриска – Eaton, Grenier и Layman (2019) посочват, че одиторските компании могат да помогнат със своята експертиза в областта на вътрешния контрол и с опита, който имат при изразяването на становища относно ефективността на вътрешния контрол върху финансовите отчети. На последните два етапа – отчитането на киберриска и независимия одит – трите автори обосновават, че счетоводителите и одиторите отново могат да се включат адекватно, тъй като разполагат с необходимите ключови компетенции (в т.ч. експертиза в сферата на финансовото отчитане, независимия финансов одит, интегрираното отчитане, одита на отчети за корпоративна социална отговорност и др.). Макар и някои от тези постановки да изглеждат леко преувеличени, трябва да се признае, че в подхода да се търсят нови и възникващи приложения на счетоводната професия има рационалност.

Мнението на професионалните организации. Според Асоциацията на международните сертифицирани професионални счетоводители

> съществува тясно съвпадение между основните качества и умения на управленските счетоводители и тези на специалистите по киберсигурност (AICPA, 2019).

Като пример в публикацията се посочва, че управленските счетоводители имат съществена роля в изготвянето на обосновката за инвестиционни

проекти, целящи повишаване сигурността на ИТ инфраструктурата, както и в ефективното управление на тези проекти. Този пример обаче не е достатъчен, за да разкрие истинските функции, които управленските счетоводители могат да изпълняват в управлението на риска. Така както управленските счетоводители партнират на мениджмънта при формулирането и изпълнението на стратегията, така те могат да партнират и при цялостното проектиране и изпълнение на процеса на управление на риска. По-конкретно, незаменима изглежда тяхната роля при: първоначалната и последваща парична оценка на риска; подбора на контролите; мониторинга на системите; оценката на ефективността на ИТ проектите; калкулирането на разходите за управление на киберинциденти с цел предявяване на искове пред застрахователите и др.

Практиката на големите одиторски компании. Различни услуги от областта на управлението на киберриска понастоящем са част от портфолиото на големите одиторски компании [5]. Тази практика недвусмислено показва, че счетоводната професия има потенциала да допринесе за по-доброто управление на киберриска в съвременните организации.

За използването на възможностите е необходима адекватна промяна във висшето образование по счетоводство

Истината е, че ролята на счетоводната професия в управлението на киберриска в бъдеще ще зависи от това, доколко успешно ще бъде реформиран съществуващият образователен модел и съответно приближен до развитието на онези компетенции, които се изискват от съвременните организации. Авторовите усилия в тази посока датират отдавна. В публикации от последните няколко години беше разработена и предложена рамка за висше образование по счетоводство, която се основава на развитието на три ключови метакомпетенции (Musov, 2016; Мусов, 2017, с. 111–127):

- метакомпетенция 1: Автентичен стил на мислене и обосноваване – включва компетенции, свързани с професионални знания, аналитично мислене, мислене в множество от перспективи и рефлексивно създаване на смисъл;
- метакомпетенция 2: Автентичен стил на действия – включва професионално поведение (професионални ценности и етика), смелост и морал;
- метакомпетенция 3: Автентичен стил на интерсубективност – работа в екип, емпатия и социална чувствителност.

Всяка една от тези метакомпетенции е изградена едновременно от две категории компетенции и качества:

> Първо, това са качествата, присъщи на човешкия характер, които следва да бъдат възпитавани у студентите с цел тяхното развитие

> не само като професионалисти, но и като личности… Второ, това са компетенциите, необходими за професионалния успех на студентите…“ (Мусов, 2017, с. 114).

Предложената образователна рамка има за цел да балансира личностното и професионалното развитие на студентите по счетоводство като допринесе за намаляването на риска от дефицитен модел на счетоводно образование. Акцентът в нея е не само върху тясно професионалните знания и умения, но и върху прехвърлимите в дългосрочен план личностни качества, както и върху интеграцията на компетенциите.

От позицията на днешния и утрешния ден предложената образователна рамка по счетоводство изглежда като стъпка в правилната посока. За това свидетелства по-скорошната публикация на IBM Institute for Business Value (2017), в която се възприема аналогичен подход на структуриране и сходно съдържание на компетенциите, необходими на специалистите по киберсигурност (вж. таблица 1). От една страна, тези компетенциите също са обособени в две групи – основни качества (общи черти на личността и поведение, придобито в резултат на учене) и умения (технически способности). От друга страна, всяка от тези компетенции има пряка проекция в предложената образователна рамка по счетоводство. Например:

- аналитичните умения и решаването на проблеми са неизменна част от метакомпетенция 1;
- нагласите за учене и етичното поведение попадат в обхвата на метакомпетениция 2;
- работата в екип и сътрудничеството са в основата на метакомпетенция 3.

Времето на традиционното и широко разпространено вярване, че висшето образование за дадена професия трябва има за основна цел развитието на компетенции, необходими единствено за нуждите на професионалната реализация на студентите, постепенно отминава. Мотивът, че по този начин се създава най-висока добавена стойност както за работодателите, така и за студентите, се оказва все по несъстоятелен. Инерцията обаче се преодолява бавно. Необходима е още много работа за реформиране на учебните планове по счетоводство и за засилване на акцента върху развитието на базовите (личностните) качества на студентите. Успехът в постигането на по-добър баланс между личностното и професионалното развитие на студентите е наистина важен – за бъдещето на завършващите професионалисти, за ролята на счетоводната професия в променящото се общество и за обществото като цяло.

Заключение

Киберрискът е сред видовете риск с най-висока вероятност за настъпване и с най-неблагоприятно влияние върху финансовото състояние на съвременните организации. Настоящата студия разглежда този риск като единство на три ключови елемента – опасност, ИТ уязвимост и неблагоприятни последици, и предлага модел за ефективно управление на киберриска, състоящ се от шест взаимосвързани етапа. В сравнение със съществуващите рамки за управление на киберриска, предложеният в студията модел има две ключови предимства. Първо, моделът е *интегриран* – обхваща всички ключови процеси – от идентифицирането, приоритизирането и оценката на риска, през въвеждането и мониторинга на системи за контрол и управлението на киберинцидентите, до неговото отчитане и неформално управление. Второ, моделът създава предпоставки за *по-уместна и по-надеждна оценка* на киберриска – акцентира едновременно върху приоритизирането на чувствителната информация и паричното оценяване на всички разходи, свързани с възникването на потенциални неблагоприятни събития.

За практическото прилагане на предложения модел е необходимо специфично професионално знание, но превес имат базовите (личностните) компетенции – аналитичните умения, уменията за решаване на проблеми, нагласите за учене, етичното поведение, работата в екип и др. Предвид спецификата на счетоводната професия, нейните представители могат да имат ключова роля в управлението на киберриска в съвременните организации. Ако целта настина е адекватно използване на сегашните и бъдещите възможности в сферата на управлението на киберсигурността, то образователният модел по счетоводство трябва да е по същество широко формиращ, а това предполага постигането на по-добър баланс между личностното и професионалното развитие на студентите.

***

Публикацията съдържа резултати от изследване, финансирано със средства от целева субсидия за НИД на УНСС по договор № НИД НИ-1/2019.

Бележки:

[1] Съгласно официалните данни на НАП (2019), са засегнати общо 5.1 млн. български граждани – от тях около 4 млн. на живи лица. Общият брой на лицата в и над трудоспособна възраст към края на предходната година в страната е 5.9 млн. (НСИ, 2019).

[2] В определени случаи тези разходи могат да подлежат на застраховане. Това зависи от нормативната уредба и от действията на засегнатата организация (за подробности вж. IRM, 2014, pp. 216–217).
[3] Очакваната стойност (EV) на разходите е средната стойност на разходите за възможните сценарии, претеглена с вероятностите за настъпване на съответните сценарии.
[4] Ползите от обучението обикновено са не само за организацията, но и за личната киберсигурност на служителите. В дългосрочен план това е важно, тъй като новите технологии (по специално интернет на нещата) все повече ще размиват границата между професионалното и личното.
[5] Например, такива услуги се предлагат от: Deloitte (вж. www2.deloitte.com/bg/en/pages/ risk/solutions/cyber-risk.html), EY (вж. www.ey.com/en_gl/cybersecurity), KPMG (вж. https://home.kpmg/ bg/en/home/services/advisory/consulting/cyber-security.html), PwC (вж. www.pwc.bg/bg/services/ras/ security.html) и други големи одиторски компании.

Референции:

Биолчева, П. (2016). Превенция на риска от изтичане на информация от търговските банки. Научни трудове на УНСС, т. 2. ИК – УНСС: 76–121.
(Biolcheva, P., 2016, Preventsia na riska ot iztichane na informatsia ot targovskite banki. Nauchni trudove na UNSS, t. 2. IK – UNSS: 76–121), достъпно на: http://unweresearchpapers.org/uploads/ResearchPapers/Research%20Papers_vol2_2016_No3_P%20Biolcheva.pdf (последен достъп: 12.12.2019).
Йонева, Е., (2018). Киберсигурността в енергийния сектор – в търсене на решения. Икономически и социални алтернативи, бр. 1. София, ИК–УНСС: 20–27.
(Yoneva, E., 2018, Kibersigurnostta v energiynia sektor – v tarsene na reshenia. Ikonomicheski i sotsialni alternativi, br. 1. Sofia, IK–UNSS: 20–27), достъпно на: https://www.unwe.bg/uploads/Alternatives/2_IA_br_1%202018_BG.pdf (последен достъп: 12.12.2019).
Моллов, Д. (2016). Управление на риска в глобалните вериги за доставка. Икономически и социални алтернативи, бр. 4. София, ИК–УНСС: 88–99.
(Mollov, D., 2016, Upravlenie na riska v globalnite verigi za dostavka. Ikonomicheski i sotsialni alternativi, br. 4. Sofia, IK–UNSS: 88–99), достъпно на: https://www.unwe.bg/uploads/Alternatives/Mollov_Alternativi_4_%202016_bg.pdf (последен достъп: 12.12.2019).
Мусов, М. (2017). Професионални компетенции и личностни качества във висшето образование по счетоводство: минало, настояще и бъдеще. (Дадена за печат: 22.02.2017 г.). София: ИК – УНСС.
(Musov, M. 2017, Profesionalni kompetentsii i lichnostni kachestva vav vissheto obrazovanie po schetovodstvo: minalo, nastoyashte i badeshte.

(Dadena za pechat: 22.02.2017 g. Sofia: IK – UNSS).
Национален статистически институт (НСИ), (2019). Население под, във и над трудоспособна възраст по области, общини и местоживеене. 12.04.2019.
(Natsionalen statisticheski institut (NSI), (2019). Naselenie pod, vav i nad trudosposobna vazrast po oblasti, obshtini i mestozhiveene. 12.04.2019), достъпно на: https://www.nsi.bg (последен достъп: 12.12.2019).
Национална агенция за приходите (НАП), (2019). Разпространени данни на НАП. Актуализирано на 09.08.2019.
(Natsionalna agentsia za prihodite (NAP), (2019). Razprostraneni danni na NAP. Aktualizirano na 09.08.2019), достъпно на: https://nap.bg/page?id=749 (последен достъп: 12.12.2019).
Adamek, D. (2019). Here's how much cybercrime can cost your company. Financial Management. AICPA, достъпно на: https://www.fmmagazine.com/news/2019/may/cybercrime-costs-201920981.html (последен
достъп: 12.12.2019).
Association of International Certified Professional Accountants (AICPA). (2019), The threat of cybercrime: How management accountants can lead the way. June 2019, достъпно на: https://insights.cgma.org/story/cybersecurity (последен достъп: 12.12.2019).
Chacko, L., Sekeris, E., & Herbolzheimer, C. (2016). Can You Put a Dollar Amount on Your Company's Cyber Risk? Harvard Business Review, достъпно на: https://hbr.org/2016/10/can-you-put-a-dollar-amount-on-your-companys-cyber-risk (последен достъп: 12.12.2019).
De Groot, J. (2019). The History of Data Breaches. Digital Guardian. January 3, достъпно на: https://digitalguardian.com/blog/history-data-breaches (последен достъп: 12.12.2019).
Deloitte, (2018). Risky business: Keeping up with the changing consumer. The Deloitte Consumer Review. September, достъпно на: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Consumer-Business/gxconsumer-review-digital-risk.pdf (последен достъп: 12.12.2019).
Eaton, T.V., Grenier, J.H., & Layman, D. (2019). Accounting and Cybersecurity Risk Management. Current Issues in Auditing. In-Press.
Ernst & Young Global Limited (EY). (2016). Path to cyber resilience: Sense, resist, react.
EY's 19th Global Information Security Survey 2016-17, достъпно на:
https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey2016pdf/$FILE/GISS_2016_Report_Final.pdf (последен достъп: 12.12.2019).
Eurostat, (2017). Social media – statistics on the use by enterprises. Eurostat Statistics Explained. Data extracted in December 2017, достъпно на:

https://ec.europa.eu/eurostat/statistics-explained/index.php/Social_media__statistics_on_the_use_by_enterprises#Use_of_social_media_by_enterprises (последен достъп: 12.12.2019).
Eurostat, (2018). Cloud computing – statistics on the use by enterprises. Eurostat Statistics
Explained. Data extracted in December 2018, достъпно на:
https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing__statistics_on_the_use_by_enterprises#Enterprises_using_cloud_computing (последен достъп: 12.12.2019).
Geneva Association – International Association for the Study of Insurance Economics (GA). (2016). Ten Key Questions on Cyber Risk and Cyber Risk Insurance. November 2016.
Zurich, достъпно на: www.genevaassociation.org (последен достъп: 12.12.2019).
Hogg, J. (2017). Why the Entire C-Suite Needs to Use the Same Metrics for Cyber Risk.
Harvard Business Review, достъпно на: https://hbr.org/2017/11/why-the-entire-c-suite-needs-to-use-the-same-metrics-for-cyber-risk (последен достъп: 12.12.2019).
Hung, M. (Ed.) (2017). Leading the IoT: Gartner Insights on How to Lead in a Connected World, достъпно на: https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf (последен достъп: 12.12.2019).
IBM Institute for Business Value, (2017). It's not where you start – it's how you finish: Addressing the cybersecurity skills gap with a new collar approach. May 2017, достъпно на: https://www.ibm.com/thought-leadership/institute-business-value/report/newcollarjobs (последен достъп: 12.12.2019).
Institute of Internal Auditors. (IIA), (2019). About the Profession, достъпно на: https://na.theiia.org/about-us/about-ia/Pages/About-the-Profession.aspx (последен достъп: 09.08.2019).
Institute of Risk Management (IRM), (2014). Cyber Risk Resources for Practitioners. IRM:
London, достъпно на: https://www.theirm.org/ (последен достъп: 09.08.2019).
Isaac, M. and Frenkel, S. (2018), Facebook Security Breach Exposes Accounts of 50 Million Users. The New York Times. Sept. 28, достъпно на:
https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html (последен достъп: 12.12.2019).
Lapena, R. (2017). Survey Says: Soft Skills Highly Valued by Security Team. October 17, 2017, достъпно на: https://www.tripwire.com/state-of-security/featured/survey-says-softskills-highly-valued-security-team/ (последен достъп: 12.12.2019).

Morgan, S., (2019). Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017-2021. Sausalito, Calif. – Jun. 10, достъпно на: https://cybersecurityventures.com/cybersecurity-market-report/ (последен достъп: 12.12.2019).
Musov, M. (2016). Beyond Vocationalism: Toward a Phenomenologically Informed Framework for Accounting Education (Working Paper Series), достъпно на: https://ssrn.com/abstract=2782203 и на http://dx.doi.org/10.2139/ssrn.2782203 (последен достъп: 12.12.2019).
National Cyber Security Centre (NCSC). (2012). 10 Steps to Cyber Security, достъпно на: https://s3.eu-west-1.amazonaws.com/ncsc-content/files/NCSC%2010%20Steps%20To%20Cyber%20Security%20NCSC.pdf (последен достъп: 12.12.2019).
National Cyber Security Centre (NCSC), (2016). Common cyber attacks: reducing the impact. Cyber Attacks White Paper. January 2016, достъпно на: https://ncsc-content.s3.eu-west1.amazonaws.com/common_cyber_attacks_ncsc.pdf (последен достъп: 12.12.2019).
Reed, J., Zhong, Y., Terwoerds, L. and Brocaglia, J., (2017). The 2017 Global Information Security Workforce Study: Women in Cybersecurity. A Frost & Sullivan White Paper.
March, достъпно на: https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/wpcontent/uploads/2019/01/women-cybersecurity-11-percent.pdf (последен достъп: 12.12.2019).
Special Eurobarometer 390. (2012). Report: Cyber Security, достъпно на: https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_390_en.pdf (последен достъп: 12.12.2019).
Sulmeyer, M. and Dugas, M. (2017). More Training Won't Reduce Your Cyber Risk.
Harvard Business Review, достъпно на: https://hbr.org/2017/11/more-training-wontreduceyour-cyber-risk (последен достъп: 12.12.2019).
The U.S. Secretary of Commerce and the U.S. Secretary of Homeland Security. (2018). A Report to the President on Supporting the Growth and Sustainment of the Nation's
Cybersecurity Workforce: Building the Foundation for a More Secure American Future.
Washington, DC. May 2018, достъпно на: https://www.nist.gov/itl/appliedcybersecurity/nice/resources/executive-order-13800/report (последен достъп: 12.12.2019).
Verizon. (2019), 2019. Data Breach Investigations Report, достъпно на: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf (последен достъп: 12.12.2019).

World Economic Forum (WEF), (2019). The Global Risk Report 2019. 14th ed. Geneva, достъпно на: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf (последен достъп: 12.12.2019).
Corera, B. (2013). Britain 'under attack' in cyberspace, BBC News, достъпно на: https://www.bbc.com/news/uk-23098867 (последен достъп: 12.12.2019).
Cyber Risk, Deloitte, https://www2.deloitte.com/bg/en/pages/risk/solutions/cyber-risk.html (последен достъп: 12.12.2019).
Cybersecurity, https://www.ey.com/en_gl/cybersecurity (последен достъп: 12.12.2019). https://home.kpmg/bg/en/home/services/advisory/consulting/cyber-security.html (последен достъп: 12.12.2019).
Интегрирано управление на информационната сигурност, PwC България, https://www.pwc.bg/bg/services/ras/security.html (последен достъп: 12.12.2019).

ПРИЛОЖЕНИЕ 1
Модел за управление на киберриска, предложен от National Cyber Security Centre (NCSC, 2012)

Десетте стъпки за управление на киберриска са разработени от National Cyber Security Centre през 2012 г. По данни на NCSC, този модел е в състояние да противодейства на 85% от случаите на нарушаване на сигурността и понастоящем се използват от повечето от компаниите в FTSE350 (350-те най-големи компании по пазарна капитализация на Лондонската фондова борса).

Стъпки	Съдържание
Въвеждане на цялостен режим за управление на риска	Оценяване на риска за системите и информацията; определяне на риск-апетита; въвеждане на режим за управление на риска, подкрепян от мениджмънта; разработване на политики за управление на риска.
Управление на привилегированите потребителски акаунти	Създаване на ефективни управленски процеси – ограничаване на броя на потребителските акаунти с привилегирован достъп, както и на самите привилегии за достъп.
Обучение и информираност на потребителите	Разработване на политики за сигурност, които да бъдат следвани от потребителите и да осигуряват приемливо ниво на сигурност. Обучение на персонала. Поддържане на информираност за киберриска.
Защита сигурността “на конфигурациите	Поддържане на сигурността на конфигурацията на цялата система. Определяне на минимално ниво на защита за всички устройства.
Защита сигурността на мрежите	Защита на мрежите от атака. Филтриране на неоторизиран достъп и злонамерен софтуер. Мониторинг и тестване на контролите за сигурност.
Превенция на зловреден софтуер	Разработване на релевантни политики и въвеждане на защити от зловреден софтуер в цялата организация.
Политика за работа извън офиса	Разработване на политика за мобилна работа и обучение на персонала за придържане към нея. Защита на данните при прехвърляне и при съхранение.
Контрол над преносимите носители “на информация	Разработване на политика за контрол на достъпа до преносимите носители на информация. Ограничаване на видовете носители и тяхното използване. Сканиране на всички носители за зловреден софтуер преди включване в системата.

Мониторинг	Създаване на стратегия за мониторинг ведно с подкрепящи я политики. Непрекъснат мониторинг на всички системи и мрежи. Анализ на регистрите с цел разкриване на необичайни активности като индикатор за кибератака.
Управление на киберинциденти	Създаване на съобщение-отговор в случай на киберинциденти и на капацитет за възстановяване в случай на киберкриза. Тестване на плановете за управление на киберинциденти. Осигуряване на специализирано обучение. Докладване за криминални случаи пред органите на реда.

Източник: Базирано на NCSC (2012)

ПРИЛОЖЕНИЕ 2
Модел за управление на киберриска, предложен от Association of International Certified Professional Accountants (AICPA, 2019)

Фази	Съдържание
Планиране	спазване на външните регулации и вътрешните политики; мониторинг и отчетност; проучване на слабостите в системата, вкл. по веригата за доставка; инвестиране в повишаване на киберсигурността; сключване на застраховка.
Подготовка	назначаване на отговорник по киберсигурността, който да разполага с достатъчно ресурси; провеждане на обучение по киберсигурност на всички служители в организацията; симулиране на кибератаки; осигуряване на антивирусен софтуер; наличие на готови съобщения-отговори до заинтересованите страни и медиите; регулярно архивиране на файлове и сигурно съхраняване.
Реакция	мониторинг на дейността с цел бързо разкриване на рисковите събития; повишаване на капацитета за документиране и оценяване на последиците; фокус върху бързия отговор на инциденти в областта на киберсигурността; бърз и ефективен от гледна точка на разходите отговор в случай на неправомерен достъп до данни с цел възстановяване доверието на клиентите; развитие на организационна култура, която допуска възможността за грешки, но разчита основно на непрекъснатото учене и възможността за бързи промени.

Източник: Базирано на AICPA (2019)

ПРИЛОЖЕНИЕ 3
Модел за управление на киберриска, предложен от Eaton, Grenier и Layman (2019)

Моделът за управление на киберриска, предложен Eaton, Grenier и Layman (2019), се базира на общи принципи на управлението на риска на предприятията и указанията на Американския институт на дипломираните експерт-счетоводители (American Institute of Certified Public Accountants) за доброволно отчитане и независим одит на киберриска.

Етапи	Съдържание/Описание
1. Идентифициране и приоритизиране на киберриска	Основна стъпка, от която зависи ефективността на целия процес.
2. Проектиране на система за контрол на киберриска	Въвеждане на ефективни контроли с цел намаляване на риска.
3. Тестване на оперативната ефективност на контролите	Регулярен мониторинг на въведените контроли.
4. Отчитане на киберриска	Комуникиране на мерките по управление на киберриска с външни заинтересовани страни, в т.ч.: описание на програмата за управление на киберриска на организацията; информация дали контролите са функционирали ефективно през отчетния период и др.
5. Независим одит на отчитането на киберриска	Независим одит от външна организация, предназначен да повиши увереността на потребителите в отчитането на киберриска.

Източник: Базирано на Eaton, Grenier и Layman (2019)

УПРАВЛЕНИЕТО НА КИБЕРРИСКА И СЧЕТОВОДНАТА ПРОФЕСИЯ

Резюме

В съвременния свят на информационни технологии (ИТ) и свързаност киберрискът е характерен за всяка една организация, а прогнозите сочат, че в бъдеще неговото ниво ще продължи да се увеличава. Това превръща ефективното управление на кибериска във въпрос от първостепенна важност. Целта на настоящата студия е на база преглед на съществуващата литература да предложи модел за управление на кибериска и да обоснове ролята на счетоводната професия в него. Разглеждайки кибериска като единство на три ключови елемента (опасност, ИТ уязвимост и неблагоприятни последици), студията предлага шест взаимосвързани стъпки за неговото ефективно управление: (1) идентифициране, приоритизиране и оценка; (2) въвеждане на система за контрол; (3) мониторинг; (4) управление на киберинциденти; (5) отчитане и независим одит и (6) неформално управление. В сравнение със съществуващите рамки за управление на кибериска, предложеният модел притежава две предимства: първо, има по-интегриран характер, и второ, създава предпоставки за по-уместна и по-надеждна оценка на кибериска, а с това и за неговото цялостно ефективно управление.
За практическото прилагане на предложения модел е необходимо специфично професионално знание, но превес имат базовите (личностните) компетенции. Предвид спецификата на счетоводната професия, нейните представители могат да имат ключова роля в управлението на кибериска. Адекватното използване на възможностите обаче налага промени във висшето образование по счетоводство.

Ключови думи: киберриск, киберсигурност, счетоводна професия, висше счетоводно образование

JEL: M40, I23, G32

CYBER RISK MANAGEMENT AND ACCOUNTING PROFESSION

Michael Musov*

Absract

In today's world of information technologies (IT) and digital connectivity cyber risk is considered inevitable for all organizations. Hence, understanding cyber risk and managing it effectively is crucial for all. This paper includes a literature review with the aim to suggest a model for cyber risk management as well as to justify the role of accountants in this model. This review leads to the conclusion that cyber risk is a unity of three elements (threat, IT vulnerability and negative impact) and suggests the following six integrated stages of its management: (1) identification, prioritization, and assessment; (2) control system design; (3) monitoring; (4) incident management; (5) reporting and assurance; (6) informal management. The incremental contribution of the proposed model with respect to the existing frameworks is in the following two differences: first, it is more integrative than the alternatives, and second, it quantifies cyber risk more relevantly and reliably than the alternatives.

To apply the suggested model cybersecurity professionals should have some technical knowledge, but the core attributes relate to their personal capabilities. Due to their specific expertise and competencies, accountants can have a key role in risk management. To benefit cybersecurity risk management, however, accounting needs to reform its higher education model.

Key words: cyber risk, cybersecurity, accounting profession, accounting higher education

JEL: M40, I23, G32

* Michael Musov, PhD in Economics, Assoc. Prof., Department of Accounting and Analysis, UNWE, email: musov@unwe.bg