ПРЕДИЗВИКАТЕЛСТВА ПРЕД ОБЕЗПЕЧАВАНЕТО НА ИНФОРМАЦИОННАТА СИГУРНОСТ В ТЪРГОВСКИТЕ БАНКИ

Проф. д-р Божидар Божинов

Резюме: Навлизането на новите информационни и комуникационни технологии в банковия бизнес радикално променя същността и характера на банковата дейност. Успоредно с конкурентните предимства и прекия икономически ефект от навлизането на високотехнологичните иновации в банковия сектор, кредитните институции се изправят и пред редица предизвикателства, едно от които е и гарантиране сигурността на предоставяните продукти и свързаната с тях информация. Основната цел на настоящото изследване е изясняване на същността, проявленията и методите за управление на информационната безопасност в търговската банка. Особен акцент се поставя върху източниците на операционен риск в търговската банка, оказващи непосредствено влияние върху потенциала за увеличаване на риска, свързан с информационната сигурност, като се разглежда ролята на банковия мениджмънт в управлението на този процес и методите и механизмите за намаляване на проявленията на разглеждания риск.

Ключови думи: банки, информационна сигурност, информационни технологии, дистанционно банкиране, онлайн банкиране.

JEL: G21.

Увод

Навлизането на новите информационни и комуникационни технологии в банковия бизнес постепенно, но същевременно и радикално променя същността и характера на банковата дейност. В исторически

план навлизането на иновативни способи за комуникация способства за намаляване на ценовите различия в географски отдалечени пазари, а по отношение на организацията, технологичните иновации съдействат за по-висока степен на интеграция и комуникация между отделните звена, както и за разширяване на продуктовата гама и използваните дистрибутивни канали.[1] Успоредно с конкурентните предимства и прекия икономически ефект от навлизането на високотехнологичните иновации в банковия сектор, кредитните институции се изправят и пред редица предизвикателства, едно от които е и гарантиране сигурността на предоставяните продукти и свързаната с тях информация[2].

Основната цел на настоящото изследване е изясняване на същността, проявленията и методите за управление на информационната безопасност в търговската банка. В този аспект обект на настоя-

[1] Вж. **Batiz-Lazo,** B., Wood, D. Information technology innovations and commercial banking: a review and appraisal from an historical perspective. Accounting and finance research unit, Manchester Business School, The University of Manchester, 2001, ISBN 0 7492 45476, p. 3.

[2] Банковата сигурност е едно от проявленията на ангажимента на банката да осигури безопасно съхраняване и управление на собствените и клиентските активи, свързаната с тях информация, както и обезпечаване на физическата сигурност и безопасност на намиращите се клиенти и служители в офисите на банката. В специализираните речници терминът „сигурност“, в контекста на банковата дейност, се дефинира като „физическа охрана, вътрешни одити и писани процедури за осигуряване на безопасност на активите на клиентите и счетоводните записи“, „защита от атака; запазване на тайна; гарантиране, че предоставените пари ще бъдат върнати“. В икономическата литература терминът обикновено се разглежда като „създаване на условия, при които опасните действия или обстоятелства отсъстват или техните възможни последици са сведени до такова ниво, при което те не са способни да нанесат ущърб в нормалното функциониране на банката, нейното имущество и инфраструктура, и да възпрепятстват постигането на поставените пред банката цели“, защита от опасности, свързани със съзнателните действията на физически или юридически лица и предназначени да нанесат щета на банката. Вж. **Шишманов**, К. Използването на съвременните информационни технологии в банковото дело – предизвикателства и реалност. Финансова стабилизация и икономически растеж. Сборник доклади, Свищов, 2000, с. 121; **Fitch**, T. Dictionary of Banking terms. Barrons's, 1997, p. 413; **Dictionary** of Banking and Finance. A&C Black Publishers Ltd, 2005, p. 319; **Лаврушин**, О.И. Банковский менеджмент. Москва, Кронус, 2009, с. 519; **Алавердов**, А. Р. Организация и управление безопасностью в кредитно-финансовых организациях. Московская финансово-промышленная академия. Москва, 2004, с. 6.

щото изследване е информационната безопасност на банковите активи, а предметът е фокусиран върху възможностите за нейното ефективно управление.

* * *

В специализираната литература няма общо възприета дефиниция и виждане за същността и обхвата на информационната безопасност[3]. В по-общ смисъл информационната безопасност обхваща всички аспекти на управлението и запазването на целостта на обработваната от дадена организация информация, независимо от нейния технически носител. В контекста на информатизацията на обществото значението на термина „информационна сигурност“ започва да се използва и в по-тесен смисъл, обхващайки единствено управлението и гарантирането на сигурността единствено на информацията в електронен вид. Успоредно с това еволюция търпи и обхватът на понятието, което от първоначалния комплекс от мерки за защита на информацията от неоторизиран достъп днес обхваща пълния комплекс от мерки за предотвратяване и отстраняване на проблемите в работата на информационните системи в съчетание с мерките по защита на информационните потоци от неоторизиран достъп и ползване.

Същевременно информационната сигурност е пряко свързана с проявлението на операционния риск в банковия сектор[4] и е пряко следствие на оперативни проблеми, организационни промени, неадекватни или липсващи процедури, липса на разделение на отговорностите, недостатъчно или неадекватно обучен персонал, нарушения на вътрешни контроли, измама или непредвидими събития, които могат да доведат до неочаквани загуби, грешки, ненавременно изпъл-

[3] За повече по въпросите, свързани с общата банкова сигурност и нейните разновидности и проявления, вж. **Божинов**, Б. Банковата сигурност – основни проявления и аспекти.// Народностопански архив, бр. 3, 2016.

[4] За повече по въпросите, свързани с банковите рискове, вж. **Божинов**, Б. Управление на рисковете в търговската банка. Библиотека „Образование и наука“, бр. 58, АИ „Ценов“, Свищов, 2013.

нение, сривове в информационните системи, пожари и бедствия, водещи до унищожаване на активи или данни[5].

Най-честите източници на операционен риск, рефлектиращи върху информационната сигурност, са свързани с[6]:

- *Персонала (човешкият фактор),* и вчастност на:
  - *Неумишлени и/или некомпетентни действия*, свързани с липса на адекватни умения и знания, неадекватно обучение, неразбиране на стандартите на работа, прилаганите методи, инструменти и процедури, невнимание, технически грешки, неадекватен контрол и др.;
  - *Умишлени действия*, свързани с неоторизирани действия при сключване на сделки, кражби, подправяне на информация в счетоводната система, подправяне на финансови и платежни документи, кражби на парични средства, хакерство, умишлено нарушаване на банкови правила и процедури, пране на пари, търгуване с вътрешна информация и други умишлени действия с цел лично облагодетелстване;
  - *Неправилно планиране и управление на персонала* – недостиг на персонал и заместването му с недостатъчно квалифициран и подготвен, отсъствие по болест, текучество и други;
  - *Засягане интересите на клиентите* чрез нарушаване на банковата тайна, огласяване на лична и/или конфиденциална информация, нарушаване интересите на доверителя и др.
- *Вътрешни процеси* – нарушения в разписаните правила, указания, процеси, политики и контролни процедури, неправилно оценяване и измерване на рисковете в резултат на пропуски или грешки в използваните модели;
- *Системи* – проблеми в информационните системи, рефлектиращи върху цялостно или частично прекъсване на операциите на банката. От своя страна те биват:

[5] Вж. **Димитрова**, Т. Вътрешният одит – ефективен инструмент на банковия мениджмънт. Библиотека Образование и наука, бр. 38, АИ Ценов, Свищов, 2013, с. 87

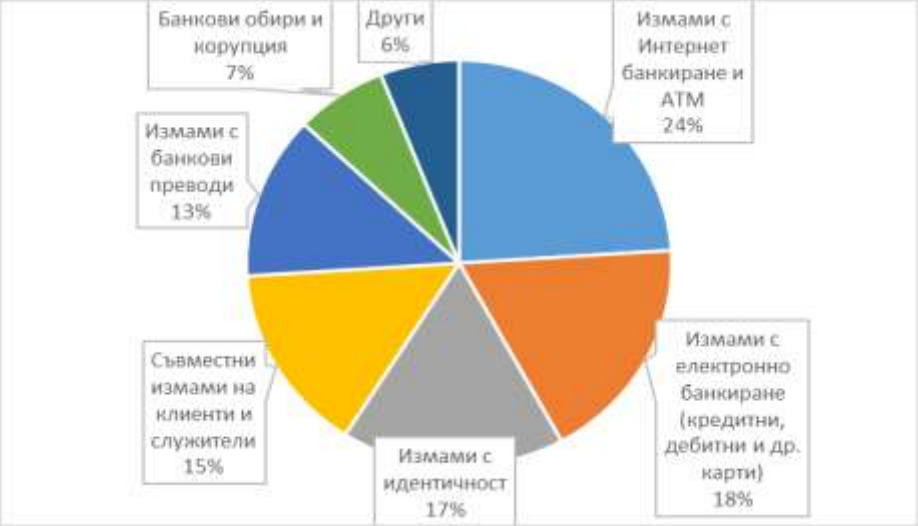
[6] За повече по въпроса вж. **Трифонова**, С. Управление на операционния риск на банките. // Вътрешен одитор, VII, N 1, 2010.

- *Общи системни рискове,* свързани с ограничаване на достъпа до системите и мрежите, неадекватни процедури за архивиране и възстановяване на данни, политика по антивирусна защита, политика по ограничаване на неоторизирания достъп до системите и др.;
- *Рискове, свързани с използвания софтуер*, породени от сривове на системите, грешки при изчисления и/или отразяване на операции или други програмни грешки в резултат на остарели и/или неадекватни технологии, неодобрен достъп до клиентски сметки и данни, проблеми с архивирането или др.;
- *Рискове, свързани с използвания хардуер*, с използването на остарели или некачествени компютърни системи, липса на резервираност на критични сървъри и хардуерни елементи, липса на системи за архивиране и възстановяване, липса на системи за аварийно захранване и др.

- *Външни фактори,* свързани с:
  - *Форсмажорни обстоятелства* – природни бедствия, пожари, вандализъм, терористични атаки и др.;
  - *Умишлени действия на трети лица* – обири, измами от името на банката, хакерски атаки, неправомерно придобиване на достъп до клиентски сметки, други предумишлени действия;
  - *Риск от доставчици на услуги* – доставчици на телефонни услуги, електрозахранване, телекомуникационна свързаност, аутсорсинг услуги и др.

Специфична особеност на банковата дейност е изискването за *конфиденциалност* относно привлечените и управляваните средства и техните собственици, което е и пряко свързано с базирани на доверие взаимоотношения между банката и нейните клиенти. Това е и една от причините, банките да са изключително мълчаливи по отношение на своите проблеми, вкл. и за инцидентите и пробивите в информационните им системи. Подобна информация обикновено изтича едва след разкриване на дадено финансово престъпление, чрез независими специализирани институции или ако самите интрудъри не

оповестят публично своя успех.[7] Тук е мястото да се отбележи, че според статистиката *едва 7% от всички извършвани банкови престъпления са осъществени с помощта на компютърни и информационни технологии*.[8]



Фигура 3. Честота на основни видове рискове, свързани с банкови измами[9]

[7] Хакери източили $71 млн. от банка през SWIFT.
http://technews.bg/article-90580.html (последен достъп 29.05.2016 г.); Хакери атакуваха сайта на гръцката централна банка.
http://news.bnt.bg/bg/a/khakeri-atakuvakha-sayta-na-grtskata-tsentralna-banka (последен достъп 29.05.2016 г.); Хакери са източвали средства от близо 100 банки по света.
http://www.capital.bg/biznes/kompanii/2015/02/16/2473701_hakeri_sa_iztochvali_sredstva_ot_blizo_100_banki_po/ (последен достъп 29.05.2016 г.)

[8] Вж. **Звезда**, И. И. К вопросу о классификации способов мошенничества в банковской сфере. // Известия Тульского государственного университета. Экономические и юридические науки, 2015, том 3-2, 97-105, с. 99.

[9] **Deloitte** - India Banking Fraud Survey - Edition II, 2015, p. 27.

Основните опити за нарушаване на информационната сигурност на банковите системи посредством присвояване, манипулиране или унищожаване на информация са продиктувани от желанието за бързо забогатяване или извършване и прикриване на друго престъпление. Те обикновено са свързани с: [10]

- *присвояване на чужда идентичност,* посредством което се осъществява кражба на авоари от съществуващи сметки на трето лице или създаване на сметки и придобиване на финансови инструменти с фалшива самоличност. И ако първите престъпления целят непосредствена кражба на пари, то вторите обикновено са част от комплексна престъпна схема за осъществяване на търговски, финансови, застрахователни или данъчни измами;
- *придобиване на конфиденциална информация с цел различни форми на шпионаж,* като мотивите най-често са свързани с проучване на бизнес или семеен партньор, както и за придобиване на вътрешна информация и използването ѝ за бъдещо обогатяване;
- *използване на банковата инфраструктура за финансови и данъчни престъпления.* Извън преките финансови, търговски и данъчни измами, в които са намесени банкови сметки на реални и/или фиктивни лица и фирми, организираната престъпност използва банковата система в опитите си за прикриване на истинския произход на придобитите от нелегална дейност парични средства и тяхното легализиране и интегриране в икономиката (процес, познат като „пране на пари“ [11]);

[10] Адаптирано по: **Lagazio**, M., Sherif, N., Cushman, M. A multi-level Approach to understanding the Impact of Cyber Crime on the Financial Sector. p. 8.

[11] Терминът „пране на пари“, като съвкупно понятие за легализиране на пари, изкарани по престъпен начин, отразява един от широко използваните пройоми на американската мафия за легализация на приходите от ротативки чрез вкарването им в банковата система като приходи от бизнес с автоматични перални машини. Счита се, че първото използване на банковата система за легализиране на доходи от престъпен бизнес е осъществено от Майер Лански (финансов съветник на Ал Капоне) по време на сухия режим в САЩ. Вж. **Storm**, A. Establishing The Link Between Money Laundering And Tax Evasion. The Clute Institute International Academic Conference Munich, Germany 2014, p. 1; **Alacer**. Happy Birthday, Anti Money Laundering! http://www.alacergroup.com/happy-birthday-anti-money-laundering/ (последен достъп 11.6.2016 г.).

- *кибер престъпленията*[12] най-често са насочени към кражба на парични средства, но могат да целят и прикриване на следи от други престъпления чрез цялостно унищожаване на цялата достъпна текуща и архивна информация в банката. Кибер тероризмът и информационната война[13], макар и различни по своя генезис и крайна цел, също представляват изключително сериозна заплаха за банковата дейност, доколкото и двете целят чрез тотално унищожение на информация и информационна инфраструктура, прекъсване на нормалните бизнес процеси и създаване на проблеми в банките, финансовата система и икономиката като цяло.

[12] В специализираната литература кибер престъпността се разглежда като традиционна престъпност, хибридна кибер престъпност, истинска кибер престъпност и платформи за кибер престъпления. *Традиционна престъпност в кибер пространството* е свързана с използването на кибер пространството като среда, предоставяща повече възможности за престъпления (напр. традиционни измами, пиратство, шпионаж, дебнене, търгуване на сексуални материали). *Хибридната кибер престъпност* се свързва основно с използването от престъпни групи на новите възможности, предоставени от Интернет (напр. кражба на идентичност, хакване, хакерство, нелегална онлайн секс търговия). *Истинската кибер престъпност* се базира на възможностите, създадени изцяло от Интернет, и се осъществява единствено в кибер пространството (напр. спам, отказ на услуга, фишинг, нелегален кибер секс). *Платформите за кибер престъпления* (напр. мрежа от ботове) се използват за улесняване на други престъпления по посочените по-горе групи. За повече информация вж. **Lagazio**, M., Sherif, N., Cushman, M. A multi-level approach to understanding the impact of cyber crime on the financial sector. p. 7.

[13] Кибертероризъм – заплаха отвъд виртуалното пространство. http://news.unabg.org/ кибертероризъм-заплаха-отвъд-вирту/ (последен достъп 11.06.2016 г.); **Мале**, П. Заплахата от кибертероризма придобива очертания. http://e-vestnik.bg/16797/zaplahata-ot-kiberterorizma-pridobiva-ochertaniya/ (последен достъп 11.06.2016 г.).

Фигура 4. Основни въздействия на проблемите с информационната сигурност върху банковите институции[14]

Основните типове щети, които банката понася в резултат на осъществени пробиви в информационната сигурност, са свързани с:[15]

- *Преки финансови щети* в резултат на кражбата на финансови средства, съхранявани и управлявани от търговската банка;
- *Непреки финансови щети* в резултат на наложени глоби от регулаторните органи, правни разходи, разходи за възстановяване на системите и информацията, прекратяване на взаимоотношенията с банката от страна на клиенти;
- *Имиджови щети,* свързани със загуба на обществено и клиентско доверие в резултат на публичното оповестяване на пробива в банковата сигурност, както и с изтичане на конфиденциална инфор-

[14] Deloitte - India Banking Fraud Survey - Edition II, 2015, p. 13.

[15] Адаптирано и допълнено по: **Lagazio**, M., Sherif, N., Cushman, M. A multi-level approach to understanding the impact of cyber crime on the financial sector. p. 11-12.

мация за осъществявани операции, обслужвани клиенти, пране на пари, участие в престъпни схеми и др.;

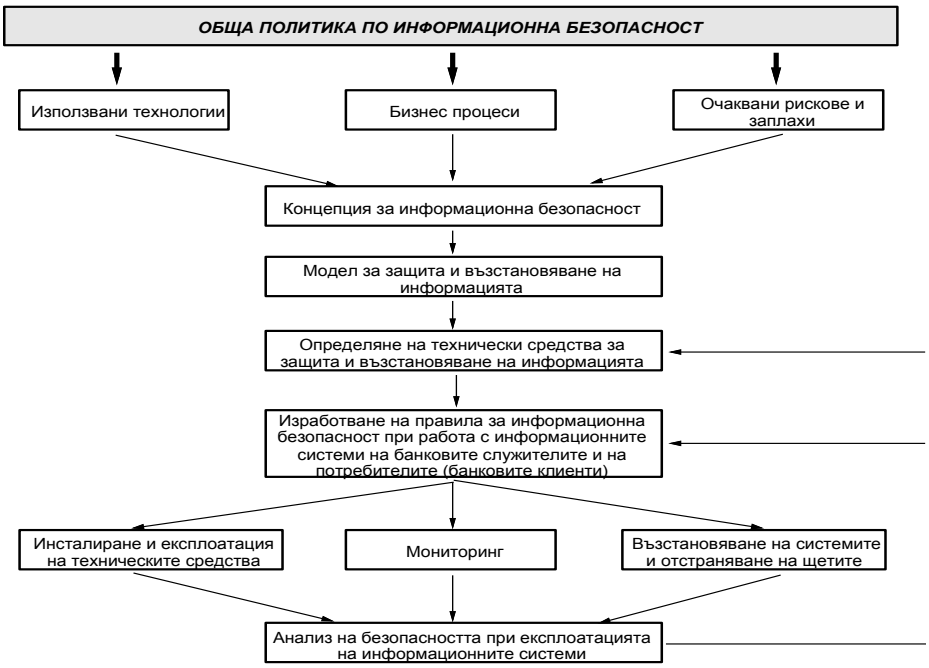
- *Пропуснати ползи* в резултат на инцидента с информационната сигурност на банката, които освен предходните две позиции обхващат и влошаване на конкурентната позиция на банката, промяна на вътрешноорганизационните приоритети, намаляване обема на работа, рефлектиращ върху намаляване на печалбата от дейността и др.;
- *Разходи за информационна защита,* които включват както разходи за информационна и комуникационна инфраструктура за предотвратяване на атаки и гарантиране на отказоустойчивост на информационните системи на банката, така и такива, свързани с въвеждането на организационни мерки по повишаване на информационната сигурност и обучението и информирането на персонала и клиентите за възникващите информационни рискове и способите за тяхното предотвратяване.

Особено важна роля в процеса на управление на информационната сигурност, като част от цялостното управление на операционните рискове, играе мениджмънтът на търговската банка.[16] В този аспект *Бордът на директорите* е натоварен с изграждането на оперативната рамка за управление на рисковете, свързани с информационната сигурност, определяне на максималния толеранс на институцията към този тип риск, както и обезпечаването на адекватно капиталово обезпечаване на поемания от нея риск. Оперативната рамка може да се разглежда като съвкупност от банковите политики и стратегии в областта на информационната сигурност, методите за идентификация, оценка и минимализирането на риска, както и организационната структура и нейните правомощия и задължения при неговото управление.[17]

[16] За повече по въпросите, свързани с управлението на банковите рискове, вж. **Божинов**, Б. Управление на рисковете в търговската банка. Библиотека „Образование и наука“, бр. 58, АИ „Ценов“, Свищов, 2013.

[17] За повече по въпросите, свързани с банковите политики, вж. **Божинов**, Б. Актуални аспекти на банковата политика. Библиотека „Образование и наука“, бр. 50, АИ „Ценов“, Свищов, 2013.

Ролята на *висшия мениджмънт* на банката в този процес е свързана със създаването на предпоставки за ефективното внедряване и прилагане на разписаните и одобрени от Борда политики, стратегии и процедури за управление на риска, свързан с информационната сигурност, както и преки отговорности по общото управление, оценка и мониторинг на цялостния процес и прилагането на коригиращи действия в случай на констатирани слабости и пропуски или промяна на вътрешната и/или външна среда. Част от мерките за повишаване на информационната безопасност са свързани и с подбора и обучението на банковия персонал, технологичното обновяване на използвания от банката хардуер и софтуер, както и прилагане на ефективни политики за вътрешен контрол.



Фигура 5. Принципна технология за осигуряване на информационната безопасност в търговската банка[18]

[18] Вж. **Тютюнник**, А. В., Турбанов А. В. Банковское дело. Финансы и статистика, Москва, 2005, с. 458.

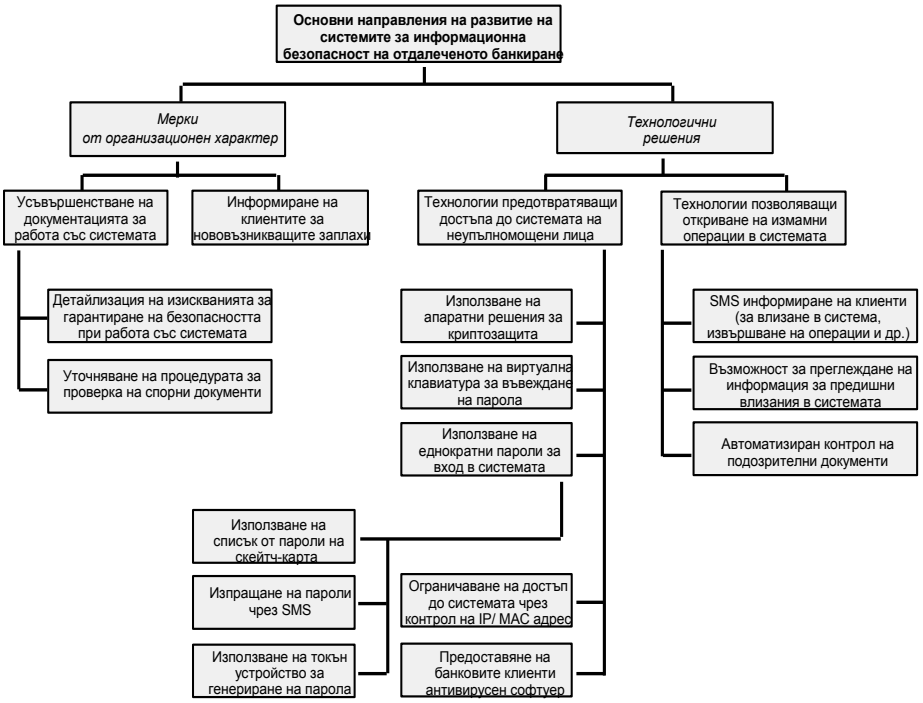
Оперативното управление на риск, свързан с информационната безопасност, обикновено е поверено на специализирано звено „Информационна безопасност“, което може да е на пряко подчинение както на ИТ отдела, така и на Комитета по управление на риска. Разбира се, осъществяване на текущ контрол върху дейността на банковите служители от техните преки началници относно спазването на установените правила и процедури и системите за вътрешен контрол е важна предпоставка за намаляване на риска от вътрешно-банкови измами или пропуски.

Доколкото рискът, свързан с информационната безопасност, е от категорията на т.нар. „чисти рискове“, т.е. той може да носи само загуби, основните подходи, свързани с неговото управление, са насочени към:

- *Избягване на риска* – този подход е приложим само за определени аспекти на този риск, които банката може да избегне (напр. отказ от предоставяне на отдалечено банкиране);
- *Поемане на риска чрез създаване на резерви*, които могат да бъдат задължителни (напр. по Наредба 8 на БНБ) и доброволни;
- *Прехвърляне на риска на трети лица,* вкл. чрез застраховане, ангажиране на външни специализирани доставчици на информационни услуги и други приложими способи;
- *Минимализиране на риска* чрез оценка, адекватни процедури за управление на процесите, отчетност и ефективен вътрешен контрол, както подбор, обучение и преквалификация на банковия персонал;
- *Диверсификация* (приложима само за някои аспекти на операционния риск, предимно свързания със системи и софтуер) чрез въвеждане на механизми за дублиране на използвани технико-технологични и комуникационни решения, външни доставчици на услуги, алтернативни способи за предоставяне на услуги и др.;

Бързите темпове на развитие на информационните и комуникационните технологии и навлизането на високотехнологичните иновации във всички сфери на човешкия живот налагат, банките да търсят адекватен инструментариум за оперативно управление и минимали-

зиране на рисковете, свързани с информационната им сигурност. Едни от най-новите подходи в тази насока включва използването на многофакторна аутентификация, геолокация, идентификация на устройства, анализ на потребителско поведение и други подобни способи.[19]



Фигура 6. Основни направления за повишаване на информационната безопасност при отдалечено банкиране[20]

[19] ACI Univercal Payment. Fighting online fraud: an industry perspective. volume 3, 2014, p. 5-6.

[20] Вж. **Визгунов**, А., Визгунов, Ар. Уровень защищенности от несанкционированного доступа как ключевой показатель качества системь дистанционного банковского обслуживания. Информационнье технологии в бизнесе, Бизнес-информатика, №2(12), 2010, с. 39.

Многофакторна аутентификация е свързана с въвеждане на многостъпков процес за еднозначна идентификация на потребителя, в който извън стандартните потребителско име и парола се използват разнообразни технически способи и устройства, съчетани с предварително предоставена от клиента лична информация (напр. любим отбор, първа кола, домашен любимец и др.), спомагаща за неговото еднозначно разпознаване от автоматизираните информационни системи на банката. По отношение на *техническите средства и устройства*, използвани за аутентификация на потребителя, банките най-често използват токъни (за генериране на случайни числа), USB устройства (в качеството му на носител на електронен подпис или друга уникална информация за идентифициране), SMS известяване (вкл. и за изпращане на еднократен потвърдителен код).

Напоследък се наблюдава тенденция в обхвата на техническите средства, банките да използват МАК адреси на устройствата на клиента (компютър, таблет, телефон) и услугите по геолокация (чрез IP адрес или GPS) за оценка на потенциалния риск от извършваната транзакция и изискване на допълнителна информация за еднозначно идентифициране на наредителя. Освен това все по-често се въвеждат и автоматизирани експертни системи, чрез които банките осъществяват анализ на потребителското поведение (напр. обичайно време на логване в системите, типични действия, обичаен размер, честота, направление и способ на плащане, използвани устройства) и на тази база търсят аномалии (т.нар. „червени флагове), които да индикират за потенциален опит за измама, вкл. и чрез откраднатa самоличност.

В последните години, като част от политиките за управление на информационната сигурност, банките започнаха да отделят особено внимание на плановете за действие при непредвидени ситуации (т.нар. Disaster Recovery Plans), като включиха в тях мерки за идентифициране и изграждане на алтернативни механизми и канали за възобновяване на услугата в случай на прекъсване (резервираност на техника, технологии, комуникационни връзки, аварийно захранване и др.), изграждане на системи за архивиране с възможност за бързо възстановяване на архивираните данни с минимална или нулева загуба на информация (изграждане на клъстерни системи, ползване на

системи за виртуализация, дублиране на данните в реално време, висока честота на архивиране, с оглед минимални загуби на данни спрямо последния момент на архивиране), както и създаване на Disaster Recovery центрове, вкл. и чрез ползване на външни доставчици или облачни услуги.

Заключение

Процесите по глобализация и дигитализация променят бавно, но безвъзвратно всички аспекти на съвременното общество, предоставяйки нови възможности и улеснения, но и изправяйки ни пред нови рискове и предизвикателства, а ролята на информацията и информационната безопасност става все по-ключова в новия дигитален свят. Търговските банки нямат никаква друга алтернатива освен да се адаптират и развиват в новите условия, а част от този процес е свързан с дигитализацията и автоматизацията на съществуващи процеси, използване на нови дистрибутивни канали за предлагането на банкови продукти и услуги и създаването на изцяло нови такива. В този аспект управлението на рисковете, свързани с информационната сигурност, се явява ново и ключово направление в развитието на банковия риск мениджмънт и цялостното управление на банковата институция.

Цитирана и използвана литература

1. Алавердов, А. Р. Организация и управление безопасностью в кредитно-финансовых организациях. Московская финансово-промышленная академия. Москва, 2004.

2. Божинов, Б. Актуални аспекти на банковата политика. Библиотека „Образование и наука“, бр. 50, АИ „Ценов“, Свищов, 2013.

3. Божинов, Б. Банковата сигурност – основни проявления и аспекти. // Народностопански архив, бр. 3, 2016.

4. Божинов, Б. Управление на рисковете в търговската банка. Библиотека „Образование и наука“, бр. 58, АИ „Ценов“, Свищов, 2013.

5. Визгунов, А., Визгунов, Ар. Уровень защищенности от несанкционорованного доступа как ключевой показатель качества систем дистанционного банковского обслуживания. Информационнье технологии в бизнесе, Бизнес-информатика, №2 (12), 2010.

6. Димитрова, Т. Вътрешният одит – ефективен инструмент на банковия мениджмънт. Библиотека Образование и наука, бр. 38, АИ Ценов, Свищов, 2013.

7. Звезда, И. И. К вопросу о классификации способов мошенничества в банковской сфере. // Известия Тульского государственного университета. Экономические и юридические науки, 2015, том 3-2, 97-105.

8. Лаврушин, О. И. Банковский менеджмент. Москва, Кронус, 2009.

9. Трифонова, С. Управление на операционния риск на банките. // Вътрешен одитор, VII, N 1, 2010.

10. Тютюнник А. В., Турбанов А. В. Банковское дело. Финансы и статистика, Москва, 2005.

11. Шишманов, К. Използването на съвременните информационни технологии в банковото дело – предизвикателство и реалност. // Финансова стабилизация и икономически растеж: Международна научно -практическа конференция, Свищов, 2000, с. 119-122.

12. Шишманов, К. Рисковете при използването на интернет банкирането и отговорността на потребителите . // Финансите и стопанската отчетност – състояние , тенденции, перспективи : Юбилейна международна научнопрактическа конференция, Сборник доклади, Т. 1., Свищов , 2013, с. 79-84.

13. ACI Univercal Payment. Fighting online fraud: an industry perspective. volume 3, 2014.

14. Batiz-Lazo, B., Wood, D. Information technology innovations and commercial banking: a review and appraisal from an historical perspective. Accounting and finance research unit, Manchester Business School, The University of Manchester, 2001.

15. Deloitte - India Banking Fraud Survey - Edition II, 2015.

16. Dictionary of Banking and Finance. A&C Black Publishers Ltd, 2005.

17. Financial Fraud Action UK. News release.

18. Fitch, T. Dictionary of Banking terms. Barrons's, 1997.

19. Lagazio, M., Sherif, N., Cushman, M. A multi-level Approach to understanding the Impact of Cyber Crime on the Financial Sector.

20. Storm, A. Establishing The Link Between Money Laundering And Tax Evasion. The Clute Institute International Academic Conference Munich, Germany 2014.

Интернет източници

21. Кибертероризъм – заплаха отвъд виртуалното пространство. http://news.unabg.org/кибертероризъм-заплаха-отвъд-вирту/ (последен достъп 11.06.2016 г.).

22. Мале, П. Заплахата от кибертероризма придобива очертания.
http://e-vestnik.bg/16797/zaplahata-ot-kiberterorizma-pridobiva-ochertaniya/ (последен достъп 11.06.2016 г.).

23. Хакери атакуваха сайта на гръцката централна банка. http://news.bnt.bg/bg/a/khakeri-atakuvakha-sayta-na-grtskata-tsentralna-banka (последен достъп 29.05.2016 г.).

24. Хакери източили $71 млн. от банка през SWIFT. http://technews.bg/article-90580.html (последен достъп 29.05.2016 г.).

25. Хакери са източвали средства от близо 100 банки по света. http://www.capital.bg/biznes/kompanii/2015/02/16/2473701_hakeri_sa_iztochvali_sredstva_ot_blizo_100_banki_po/ (последен достъп 29.05. 2016 г.).

26. Alacer. Happy Birthday, Anti Money Laundering!
http://www.alacergroup.com/happy-birthday-anti-money-laundering/ (последен достъп 11.6.2016 г.).

БИЗНЕС управление

Стопанска академия
„Д. А. Ценов“ – Свищов

Година XXVI, кн. 3, 2016

СЪДЪРЖАНИЕ

Дадено за печат на 15.09.2016 г., излязло от печат на 21.09.2016 г., формат 70x100/16, тираж 150

ISSN 0861 - 6604

БИЗНЕС управление

ИЗДАНИЕ НА
СТОПАНСКА АКАДЕМИЯ
„Д. А. ЦЕНОВ" - СВИЩОВ

3/2016

БИЗНЕС управление 3/2016

КЪМ ЧИТАТЕЛИТЕ И АВТОРИТЕ НА СПИСАНИЕ „БИЗНЕС УПРАВЛЕНИЕ"

Списание „БИЗНЕС управление" **публикува изследователски статии, методологически и методически разработки и прегледи, рецензии, опит.**

1. Обем:
Статии: минимум - 12 страници; максимум - 25 страници;
Прегледи, рецензии, опит: минимум - 5 страници; максимум - 10 страници.

2. Депозиране на материалите:
- на хартиен носител и в електронен вид (по E-mail и/или на CD);

3. Технически характеристики:
- изпълнение Word 2003 (минимум);
- размер на страницата - A4, 29-31 реда и 60-65 знака на ред;
- разстояние между редовете 1,5 lines (At least 22 pt);
- шрифт - Times New Roman 14 pt;
- полета - Top - 2.54 см.; Bottom - 2.54 см; Left - 3.17 см; Right - 3.17 см;
- номерация на страницата - долу вдясно;
- текст под линия - размер 10 pt;
- графики и фигури - Word 2003 или Power Point.

4. Оформление:
- наименование на статията, име на автора, научна степен, научно звание - шрифт Times New Roman, 14 pt, с големи букви Bold - центрирано;
- наименование и адрес на месторабoтата; телефони за контакти и E-mail;
- резюме на български език в обем до 15 реда; ключови думи - от 3 до 5;
- **JEL** класификация на публикациите с икономически характер (http://ideas.repec.org/j/index.html);
- основен текст (изложение);
- таблиците, графиките и фигурите се вграждат софтуерно в текста (да позволяват езикова корекция и превод на английски). Цифрите и текстът вътре в тях се изписват с шрифт Times New Roman 12 pt;
- формулите се създават с Equation Editor;

5. Правила за цитиране под линия:
При цитиране да се спазват изискванията на **БДС 17377-96 Библиографско цитиране**, поместени тук: http://www.uni-svishtov.bg/?page=page&id=71
Всеки автор носи отговорност за отстояваните идеи, съдържанието и техническото оформление на своя текст.

6. Контакти:
Главен редактор: тел.: (++359) 631-66-397
Зам.-главен редактор: тел.: (++359) 631-66-425
Стилов редактор и ПР: тел.: (++359) 631-66-335
E-mail: jtananeeva@uni-svishtov.bg
Адрес: Стопанска академия „Д. А. Ценов", ул. „Е. Чакъров" № 2, Свищов, България