ПРЕВЕНЦИЯ НА РИСКА ОТ ИЗТИЧАНЕ НА ИНФОРМАЦИЯ ОТ ТЪРГОВСКИТЕ БАНКИ

Петя Биолчева[1]

Увод

В условията на висока дигитализация на икономика трансферът на данни в киберпространството е на рекордни равнища. В търговските банки се осъществяват транзакции на огромно количество файлове за изтегляне и спестяване на различни суми. Банките притежават чувствителни данни за клиенти, бизнес партньори, регулатори и акционери, които изискват високо ниво на тяхната защита.

Практиката показва, че банковият сектор често става обект на различни информационни атаки, а понякога и жертва на масивна загуба на данни, както и изтичания на информация за банкова тайна и значителни количества парични средства. Това, от своя страна, вреди сериозно на конкурентоспособността и репутацията на атакуваната банка. От тук произтича и **актуалността на настоящия труд.** Банковата информация трябва да бъде защитена от неоторизиран достъп. Търговските банки трябва да предприемат навременни мерки за идентифициране, анализиране, въздействие и контрол на риска от изтичане на информация.

Превенцията от изтичане на банкови данни е насочена към ограничаване на загубата на чувствителна информация. За успешното й прилагане се изисква значителна подготовка и усърдна текуща работа по осигуряването й. Банките, които искат да гарантират високо ниво на защита на чувствителната информация, трябва да бъдат подготвени за значителни усилия. Това изисква идентификация на рисковете, въздействията и стъпките за смекчаване на рисковите заплахи, заедно с подходящи мерки за управление и осигуряване на високо равнище на информационна защита (Antony, Melek, 2010, p. 5). Превенцията на рисковете от изтичане на информация осигурява възможността за предприемане на навременни мерки, преди проявата на дадено рисково събитие. Това, от своя страна, би гарантирало на банките поддържане на висока репутация.

[1] Петя Биолчева е доктор по икономика, асистент в кат. "Индустриален бизнес" на УНСС; e-mail: p.biolcheva@unwe.bg

Темата на студията се отличава с недостатъчна разработеност в теоретичен и практико-приложен аспект. В литературата е добре разработен въпросът относно банковите институции и източниците на изтичане на информация поотделно, но е слабо засегнато обвързването им, още повече, що се отнася до динамиката на информационните технологии и ежедневната поява на нови рискове в полето на изследваната тематика.

Обект на изследване в настоящия труд е извадка от банки, работещи на територията на страната ни. От гледна точка на темата, обектът на изследване е интересен поради важността на банковите институции в икономическия живот на всяко физическо и юридическо лице. Нарушаването на основните бизнес процеси в банките, породено от проявата на риск, свързан с изтичане на информация, би нарушило както банковата репутация, така и интересите (финансите) на клиентите на банката. По-важните характеристики на търговските банки (ТБ) като обект на изследване са:

- ТБ е юридическо лице (АД), което извършва публично привличане на влогове и други възстановими средства и предоставя кредити или друго финансиране за своя сметка и на собствен риск;
- ТБ изпълняват функции на финансово посредничество и обслужване на финансови сделки и плащания в условията на значителен риск;
- От изключително значение е стабилността на ТБ, осигурявана чрез високи изисквания към капиталовата им адекватност, тяхната сигурност (в т.ч. информационната) и професионалното им управление;
- ТБ са основен елемент на банковата система и имат решаващ принос за генериране на доверие в обществото към банките и цялата банкова система.

Предметът е съсредоточен върху това да покаже как се осъществява превенция на рисковете, свързани с изтичането на информация от банките. Изтичането на информация е умишлено или неоторизирано пренасяне на чувствителни данни от дадена организация към външни приемници.

Целта на изследването е да бъде разкрита спецификата при превенцията на риска от изтичане на информация, като за нейното постигане са поставени следните **задачи**:

- Да бъде извършена идентификация на рисковете, свързани с изтичането на информация в търговските банки;
- Да бъдат установени формите и тежестта на последствията от сбъдването на рисковете;
- Да бъдат предложени средства за превенция на установените рискове.

Настоящият научен труд се подчинява на **тезата**, че търговските банки у нас полагат значителни усилия при управлението на риска от изтичане на информация, въвеждайки все по-усъвършенствани информационни защити

и технологии. Въпреки това посоченият риск намира все по-нови проявления. Той се запазва на високо равнище и по отношение на вътрешните, и на външните източници, които го провокират.

За постигане на изследователската цел и при решаването на задачите на труда са използвани редица **методи** за теоретичен анализ, анализ на нормативната уредба, сравнителен анализ, статистически методи, емпирично проучване под формата на анкети и др.

По същество **основните ограничения** на изследването произтичат от формулираните обект, предмет, цел и задачи на труда. Те определят неговата концептуална рамка и позволяват да се задълбочи цялостното изследване. Поради широкия спектър на риска, отнасящ се до изтичане на информация, се поставя ограничението да бъдат разгледани само основните групи заплахи, провокиращи проявата на този риск. Поради техническата специфика на средствата за информационна защита те няма да бъдат разглеждани.

Актуалността на разглежданата тематика стимулира банките редовно правят индивидуални проучвания за състоянието на посочения риск. Той е обсъждан и на конференции в страната, например: "X Регионална конференция по информационна сигурност и съхранение на данни, София, 2011 г.", където са разгледани въпроси като вътрешни заплахи, свързани с изтичането на информация, канали за изтичане на информация и др.

1. Търговски банки

Банка (кредитна институция) е юридическо лице, което извършва публично привличане на влогове или други възстановими средства и предоставя кредити или друго финансиране за своя сметка и на собствен риск (Закон за кредитните институции, 2006, чл. 2).

В закона за кредитните институции са дефинирани основните дейности, с които банките могат да се занимават, а именно: извършване на платежни услуги, финансов лизинг, гаранционни сделки, търгуване с чуждестранна валута и благородни метали, парично брокерство, придобиване на вземания по кредити и друга форма на финансиране (факторинг, форфетинг и други), издаване на електронни пари, придобиване и управление на дялови участия и др.

Така – посредством дейността си – търговските банки стоят в центъра на стопанския живот на страната. Те са "работното колело" на финансовата система. Причините за това са:

- оперират с чужди парични средства, привличайки и едновременно с това отразявайки доверието на различни категории собственици;
- спомагат за създаването на икономически агенти (субекти) и икономически структури;

- извършват многобройни и разнообразни услуги;
- имат постоянен стремеж към реализиране на доходи и печалби (Радков, Михайлов, 2002, с. 35-37).

Банката се учредява като акционерно дружество и за нея се прилага Търговският закон. Минимално необходимият внесен капитал при учредяването на банка не трябва да е по-малък от 10 млн. лева. Банката може да открива повече от един клон в отделно населено място, включително в населеното място, където е нейното седалище. За извършването на банкова дейност се изисква лиценз, издаден от БНБ. Към момента в България осъществяват дейност 22 лицензирани търговски банки.

Банка, лицензирана в държава – членка на ЕС, може да извършва дейност на територията на Република България чрез клон, ако дейностите й се припокриват с тези, приети в нашето законодателство и след като БНБ бъде уведомена за това от компетентния орган, издал лицензия. Към момента в България осъществяват дейност 6 клона на чуждестранни банки.

Наред с издаването на лицензи, Централната банка може и да ги отнеме. До тези действия се прибягва, когато: търговската банка не започне да извършва дейност в срок от 12 месеца от издаването на лицензия; същата е извършила нарушения по Закона за кредитните институции; преустановила е извършването на дейност за срок повече от 6 месеца; Българската народна банка е установила, че влоговете в банката са неналични и др. (Закон за кредитните институции, 2006, чл. 7-13).

Търговските банки заемат най-голям относителен дял в банковата система. Те са и обект на изследване на настоящия труд. В своята дейност търговските банки се стремят така да организират привличането на депозити и отпускането на кредити, че в крайна сметка да максимизират ефекта от дейността си и да реализират печалба. Маржът, представляващ разликата в лихвените проценти по депозитите и кредитите, е основен източник на банкова печалба.

В процеса на цялостната си дейност, свързан с формирането на парични активи и набирането на определена кредитна активност, банките се явяват финансови посредници.

Търговските банки изпълняват две основни функции – осигуряване на финансово посредничество на физически лица, домакинства, юридически лица и правителството и обслужване на финансови сделки и плащания. Те изпълняват изключителни функции по първоначалното привличане на депозити и на спестявания с цел преобразуването им в инвестиции срещу определена печалба за банката. Депозитите на клиенти на банката се концентрират като пасиви в баланса й, т.е. разполагаем парично-кредитен ресурс, който банката използва за композиране на големи, разнообразни по

възможности портфейли от банкови активи. Активите на банката са нейните вземания, възникнали от предоставяне на пари под формата на кредити, покупки на ценни книжа и др.

На практика посочените функции се свеждат до два типа банкови операции – пасивни и активни. Банките се различават от останалите финансови посредници по това, че те са единствените депозитонабиращи институции. Това има пряка връзка с проблематиката на информационната сигурност и тематиката, разглеждана в настоящия труд.

Разглеждането на банките от гледна точка на обвързаността им с изтичането на информация предизвиква интерес от научна и практическа гледна точка. Банките са сред организациите с най-висок рисков профил що се отнася до честотата на проявление и тежестта на последствията от риска, свързан с изтичане на информация. Проявлението на риска тук рефлектира в директни финансови загуби, загуби в активите на банковите клиенти, отлив на клиенти, а също и сериозни репутационни щети.

2. Видове информация, с която работят търговските банки

Банката създава, поддържа и осъвременява информационна система, която съдържа:

1. устава и другите вътрешни правила с всички изменения и допълнения в тях;
2. определени от БНБ данни за акционерите;
3. книги с протоколи от заседанията на общото събрание на акционерите и на другите органи за управление;
4. счетоводна информация, отразяваща ясно и вярно вида, размера и основанието на сключените сделки и отражението им върху финансовото състояние на банката, от която да може да се установи дали банката извършва дейността си в съответствие с разпоредбите на Закона за кредитните институции;
5. информация по клиенти с данни за сключените с тях или за сметка на тях сделки и за кредитните и дебитните им салда;
6. общите условия, които банката прилага по банковите си сделки, измененията и допълненията в тях;
7. подробна документация за финансовите договори, по които банката е страна;
8. информация, изисквана по Закона за кредитните институции и различни поднормативни актове на БНБ.
9. Банката създава и поддържа досието за всеки кредит с данни за клиента, основанието, условията и размера на кредита и неговото обезпечение, решението на компетентния орган за отпускане на кредита и всички дру-

ги данни, свързани със сключването и изпълнението на договора (Закон за кредитните институции, 2006, чл. 67, 68).

Предвид важността на информацията, с която работят банките, тя се класифицира като банкова тайна. Банкова тайна са фактите и обстоятелствата, засягащи наличностите и операциите по сметките и влоговете на клиентите на банката. В тази връзка всички банкови служители, имащи отношение към работата с тази информация, подписват декларация за пазене на банковата тайна при встъпване в длъжност, при изпълнение на възложената работа и след преустановяване на трудовите правоотношения.

Банковите служители могат да нарушат това условие само при предвидени от закона случаи, свързани със:

- съдебни решения за изясняване на определени обстоятелства при наличие на данни за извършено престъпление;
- необходимо налагане на запори върху банкови сметки за обезпечаване на установени вземания;
- целите на разкриването и разследването на престъпления от Министерството на вътрешните работи;
- наличие на данни за организирана престъпна дейност или за изпиране на пари.

Практиката показва, че с най-високо ниво на риск от кражба са следните групи данни:

- банкова информация – лични данни за клиентите и финансовите им данни, включително номера на кредитни карти и данни за банкови сметки и техните наличности;
- системни и потребителски мрежови пълномощия като например пароли и сертификати;
- оперативни методики;
- правни данни относно текущи или планирани съдебни или договорни действия;
- частни документи на другите потребители, съхранени на фирмени компютри;
- стратегически данни, включително комуникациите на ръководен и изпълнителски персонал (Data Theft, 2009, p. 2).

Поради големия обхват на информацията, с която работят банките, и различната степен на нейната важност тук се поставя следното ограничение. Информацията, чиято превенция се търси с разработване на настоящия труд, е:

- Банкова тайна, засягаща информацията по сметките на клиентите на банката;
- Чувствителната информация в банката, която съдържа данни на банката относно организацията на работния процес, мерките за сигур-

ност в банката, договорните й отношения с различни контрагенти и още редица други данни, свързани с дейността й, които се определят като конфиденциални.

3. Информационна сигурност

Информацията може да бъде дефинирана като съвкупност от нефизически характеристики, определящи даден обект. Тези характеристики определят свойствата и поведението на обекта (например клиентски акаунт). В същото време неразривна част от информацията са данните. Те дават количествен израз на характеристиките на обекта.

Понятието информационна сигурност е свързано със съхраняването, обработката и предаването на информация. Под информационна сигурност се разбира защитата на информацията и поддържащата я инфраструктура от случайни или преднамерени въздействия от естествен или изкуствен характер, които могат да нанесат неприемлива вреда на собствениците или на ползващите информацията, както и на поддържащата инфраструктура. Основната цел на информационната сигурност е да обезопаси и защити информацията или да намали до минимум нейната загуба (Social Dude).

Според ISO/IEC – 27001:2005, информационната сигурност е опазване на конфиденциалността, целостта и наличността на информацията, като допълнително могат да се включат и други свойства като автентичност, отговорност, удостоверяване без право на отказ и надеждност (ISO/IEC 27001:2005 Information technology, p. 7).

Заплахите за сигурността на информацията приемат най-различна форма. Някои от най-честите са: софтуерни атаки, кражба на интелектуална собственост, кражба на самоличност, кражба на устройство или информация, саботаж и манипулиране на информацията. Повечето хора са изпитали някакъв вид софтуерна атака: разните вируси, червеи, фишинг и троянски коне са примери за такива атаки.

Информационната сигурност е изправена пред динамично непостоянство, неопределеност на средата и нееднозначност на заплахите. Сигурността на информацията изисква добро осигуряване на банковите данни, което предполага те да отговарят на следните критерии:

- споделимост и своевременност;
- сигурна достъпност;
- сливане, точност и пълнота;
- обективност, достоверност, надеждност (Семерджиев, 2004, с. 24).

На това място следва да бъде дефинирано какво може да се случи при въздействие върху информацията. Вариантите при сбъдване на риска, отнасящ се до осъществяване на пряка връзка между източника на информацията (банката) и получателя (клиента) на информацията, могат да бъдат:

- прекъсната,
- подслушвана,
- модифицирана,
- изфабрикувана информация (Павлов, 2013).

За да отговори на посочените по-горе критерии, банковата информация трябва да бъде разграничена в различни модули: данни в покой, данни в движение и данни в употреба. За всеки модул на състояние на данни се изискват различни решения. За работата с всеки модел се изискват и различни мерки за осигуряване на информационна сигурност.

- **Данните в покой –** важно за този модул от данни е възможността те да се идентифицират и да се причислят към специфичния вид информация, която се съхранява в банката (например банкова тайна). Това означава, че всеки оторизиран банков служител трябва да има възможността лесно да я търси и идентифицира и да открива конкретни части от информация (например за дадена кредитна карта).

Данните в покой са данни, които се съхраняват в рамките на информационната инфраструктура, например: сървъри, бази данни, споделени файлове, интернет сайтове, работни станции, лаптопи, мобилни устройства, преносими памети и др. Данни в покой могат да се съхраняват и чрез външни разширения на информационната инфраструктура като облак за съхранение.

- **Данните в движение (в мрежата)** – при този вид информация се изисква системата за информационна сигурност на банките да осигурява извършване на постоянен анализ на мрежовия трафик. Когато файловете са изпратени от страна на друга мрежа, те обикновено са разделени на пакети. За да се запознае с информацията, която се изпраща по мрежата, банковата система за информационна сигурност трябва да извърши пасивно наблюдение на мрежовия трафик, да познае правилните информационни потоци, за да улови и да групира събраните пакети, да реконструира файловете, проведени в потока от данни, и след това да извърши анализ, който се прави въз основа на данните в покой. Данните в движение са данни в режим на транзит, преминаващ през вътрешните мрежи и външния свят.
- **Данните в употреба –** те са може би най-голямото предизвикателство пред информационната банкова сигурност. Това са данни, по които в момента се работи или се използват от системата в определена точка

от времето. Тяхната защита се свързва предимно с мониторинга на данните, произтичащи от действия, предприети от банковите служители на техните индивидуални работни места, независимо дали това се свързва с копиране на данни на флаш-памет, изпращане на информация към принтер, или дори изрязване и поставяне на определена информация между различни приложения.

За да осигури превенция от изтичането на информация, банковата система за информационна сигурност трябва да е в състояние да се справя рационално и с трите модулни състояния на информацията. Това налага изграждането на интегрирана с генералната управленска функция защита на информацията (Antony, Melk, 2010, p. 6).

4. Методична схема за превенцията на риска от изтичане на информация

Фигура 1. Превенция на риска от изтичане на банкова информация

Анализирайки риска от изтичане на информация в банките, е необходимо да се обърне внимание на бизнес средата на конкретната банка и да се направи анализ на източниците (каналите) за изтичане на информация. Всички те са насочени към атака върху банковата и чувствителната информация. Банковата информация съдържа цялата информация за банко-

вите клиенти и техните финансови активи. Чувствителната информация се отнася до осъществяване на нормалните бизнес процеси в банката, в това число специфика на работата, договори с контрагенти, мерки за сигурност на работните процеси и т.н. Сбъдването на потенциално рисково събитие би довело и до потенциални щети в две основни направления – финансови и репутационни. В същото време системата за банковата информационна сигурност е необходимо да насочи усилията си в подходящи и навременни мерки по превенция на споменатият риск. Ако превенцията е целесъобразна и ефективна, то тя би елиминирала или поне понижила честотата и тежестта от последствията на риска, свързан с изтичане на информация.

5. Канали за изтичане на информация

Изтичането на информация е неоторизирано предаване на данни (или информация) от рамките на една организация към външна дестинация или получател. То може да бъде извършено по електронен или физически път. Изтичането на информация е както неумишлено, така и злонамерено (Gordan, 2007, p. 5).

За да бъде осъществена добра превенция на риска на това място (в съответната банка) следва да бъде извършена идентификация на източниците на изтичане на информация.

Загубата на информация, породена от изтичане, може да се осъществи по два основни начина – от вътрешни или от външни източници. Практиката показва, че почти половината от информацията, която изтича от търговските банки, е от вътрешни източници.

5.1. Изтичане на информация от вътрешни източници

За изтичането на информация от вътрешни източници е характерно, че в голямата си част то се свързва с непреднамерени действия от страна на банковите служители. Тук се имат предвид главно различни вируси, които се прихващат чрез електронната поща, при посещение в различни блогове и сайтове. Не бива да бъде пренебрегван и рискът от преднамерени действия на банкови служители.

Най-честите случаи, които подтикват банковите служители към изнасяне на информация, се наблюдават при:

- внезапно напускане на служител с достъп до чувствителни данни;
- преминаването на служител в конкурентна банка;
- служител, който бива поставен под въздействието на различни зависимости, като принуда и изнудване;
- уволнен служител;

- служител, имащ лични отношения с лица в конкурентни банки;
- служител, имащ лични отношения с журналисти, и т.н.

По информация, получена от разследване на тайните служби на САЩ, нарушителите, склонни към изнасяне на информация, са предимно мъже (96%). По-голямата част от тях са заемали предимно длъжности, свързани с технически позиции (86%). Последствията от техните нарушения са свързани не само с изнасяне на информация, но и със саботаж на информационната система за сигурност (Keeney, 2005).

Възможни индикатори за потенциалните намерения за кражба на данни от служител се наблюдават в следните случаи:

- искане за отдалечен достъп – без основателна причина, или ако дългогодишен служител внезапно поиска такъв, без да има промяна в работните му задължения;
- внезапно нарастване на големината на имейлите, които изпраща даден служител;
- мащабна издирвателна дейност по файлове в сървър системата;
- работа в нерегламентирано работно време, късно вечер или през почивните дни;
- ако конкурентни банки необичайно бързо пуснат на пазара продукти или услуги, по които се работи в съответната банка, и др. п.

Потенциални доказателства за кражба на данни могат да бъдат:

- изпратени съобщения в електронната поща;
- истории за достъп до файловете, които показват наличието на ключови файлове на външни устройства;
- файлове и документи "метаданни", показващи скорошен достъп;
- файлове и записи в регистъра, които показват наличието на външни запаметяващи устройства;
- временни файлове и записи в регистъра, показващи достъп до ключови документи;
- наскоро създадени "Zip"-файлове, използвани за компресиране на откраднатите данни;
- сървърни дневници за отдалечен достъп, показващи часове и дати на достъп до ключови сървъри (Data Theft, 2009, p. 4).

Банковата практика показва, че най-честите случаи на изтичане на информация са свързани с непреднамерени действия. Част от тях са илюстрирани във фиг. 2:

Фигура 2. Непреднамерено изтичане на информация

Източник: Data Loss Prevention keeping your sensitive data out of the public domain, Insights on governance risk and compliance, 2011, p. 7.

С най-висока степен на риск от загуба на информация за банките се оказват:

- Приложенията за моментални съобщения "Instant Messaging" като Skype, GoogleTalk, Viber и много други. Част от банките позволяват на определена група служители (обикновено намиращи се на по-високо йерархично равнище) да получат достъп от техните работни станции или лаптопи до такъв род приложения. С тях може лесно да се осъществи трансфер на данни и файлове. Тук се крие и рискът даден служител да разгласи чувствителна информация. Друг риск представлява възможността тези приложения да бъдат атакувани от зловреден софтуер.
- Служебните имейли. Широко разпространена е комуникацията посредством електронна поща – както в предаване на служебна информация между отделните служители и контрагенти, така и между слу-

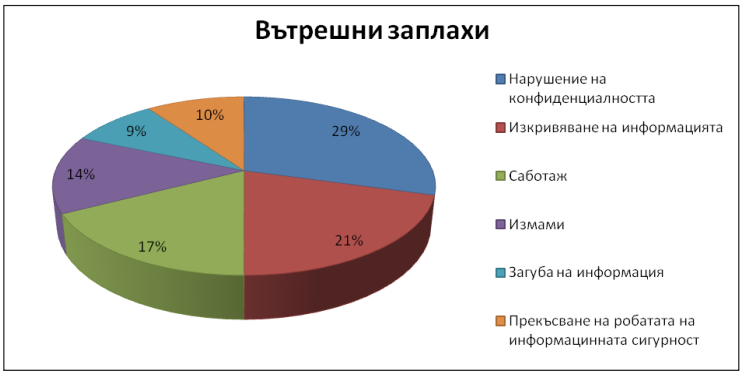
жителите и клиентите на банката. Най-често използвани за служебна кореспонденция са пакетите на Microsoft Outlook, Lotus Notes, Eudora, и т.н. Тук съществува рискът даден служител да изпрати неоторизиран имейл с поверителен документ към неоправомощени лица. Служителят може също така да извърши компресиране и/или криптиране на файлове, или да ги вгради в рамките на други файлове. Друг риск, свързан по-скоро с грешка по невнимание, е възможността служител да прикачи грешен файл или да избере грешен получател в електронна поща.

- Лична електронна поща. Възможността за използване на личните имейли представлява още един риск за изтичане на поверителна информация. При използване на личната поща рискът от това да бъде заловен злонамереният служител е по-малък, отколкото при ползването на служебната такава.
- Блогове. Друга заплаха са определени уеб сайтове (Blogs), където хората могат да излагат своите мисли, коментари, мнения по даден въпрос. Блоговете могат да бъдат индивидуални или публични сайтове, в които могат да се включат хиляди хора. Те са обект на риск от гледна точка на това, че някой може да пусне поверителна информация – просто, чрез влизането в блога си (Data Theft, 2009, p. 12).
- Злонамерените уеб страници. Уеб сайтове, които или са компрометирани, или са умишлено злонамерени, са друга рискова група, застрашаваща банковата информация. Съществува риск компютърът на служителя да бъде заразен със зловреден софтуер, като се посети уеб страница, съдържаща злонамерен код, от браузър, който съдържа уязвимост. Зловреденият софтуер може да бъде под формата на различни вируси, троянски коне и т.н. Така се повишава рискът от кражба на данни (Parizo, 2007).
- Протокол за пренос на файлове *(File Transfer Protocol FTP)*. Представлява мрежов протокол от тип потребител-сървър, даващ възможност за обмяна на файлове между машини, свързани в локална мрежа или в Интернет. Протоколът за пренос на файлове използва комуникация между потребител и сървър. Потребителят влиза чрез специално разработена програма, която предоставя лесен начин за използване на възможностите за комуникация. Протоколът предоставя възможността за изпълняване на операции на сървъра като показване на съдържанието на директории, смяна на директорията, създаване на директории и триене на файлове. Тук съществува рискът преди всичко от умишлено унищожаване и/или изтичане на данни от действията на оторизиран банков служител.

- Копиране на хартиен носител. Когато дадено лице желае да изнесе чувствителна информация, а търговската банка е въвела електронни контрамерки, съществува рискът служителят да разпечата данните и да ги изнесе физически.
- Камери. Отново, ако дадената банка е изпълнила набор от защитни мерки за предотвратяване на изтичането на информация по електронен път, друга установена възможност за злонамерените вътрешни лица е те да направят цифрови снимки с мобилните си телефони.
- Неадекватно съхранение на архивни единици. Ако за папките с хартиени носители и файловете липсва подходяща защита (чрез потребител/група привилегии и т.н.), те стават лесна плячка за копиране на данни от мрежово устройство и локална система. Потребителят може да копира този файл на сменяеми носители или да го изпрати по електронната поща.
- Флаш памет. Широко използван инструмент за пренасяне на данни. Трансферът на поверителна служебна информация върху този род устройство представлява лесен начин за изтичане на информация. Тук стои въпросът пред банковите специалисти по информационна сигурност кои портове за USB реално могат да бъдат разрешени за ползване от служителите и доколко това се налага от длъжността им. Друг риск с преноса на информация с флаш памет е възможността самата флашка да бъде изгубена или заразена със зловреден софтуер. Други устройства, попадащи в тази рискова група, са преносими твърди дискове, музикални устройства, дори CD и DVD.
- Неадекватна защита на файлове. Ако в банката липсва подходяща защита чрез дефиниран достъп за определени служители, информацията става лесна за манипулиране и злоупотреби чрез методите, обсъдени по-горе.
- Скриване в *SSL*. С цел прикриване (замаскиране) на данни, банковият служител може да се опита да използва услуга на публично прокси чрез SSL връзка (често наричано Заобикаляне чрез Прокси). Те достигат до прокси услугата чрез браузъра, въвеждат URL сайта, който искат да посетят, и данните в цялата сесия след това се кодират. Така, защитната функция на информационната система за защита няма да бъде в състояние да разгледа данните, тъй като те ще бъдат криптирани. Следователно, чувствителна информация може да изтече чрез тази среда, без това да бъде открито.

По доклад от "X регионална конференция по Информационна сигурност и съхранение на дини" 53% от изтичанията на информация са свързани с

неправилната организация на работните процеси; 46% – с незаинтересоваността на персонала, и едва 1% – със зла умисъл.



Фигура 3. Статистика на реализираните вътрешни заплахи по видове

Източник: Димитров, С., Доклад "Сигурност на информацията и до какво може да доведе бездействието при нейното управление", X регионална конференция по Информационна сигурност и съхранение на данни, София, 2011.

Фигура 4. Статистика на каналите за изтичане на информация по видове (Димитров, 2011)

Източник: Димитров, С., Доклад "Сигурност на информацията и до какво може да доведе бездействието при нейното управление", X регионална конференция по Информационна сигурност и съхранение на данни, София, 2011.

5.2. Изтичане на информация от външни източници

Тази група рискове е свързана преди всичко с атаките на злонамерени лица, целящи придобиване на финансовите активи на банката. Основните групи рискове, попадащи в тази категория, са:

- Кражба на данни от престъпници. Тази група рискове е свързана най-вече с кражба на информация за кредитни карти. През последните години все повече зачестяват случаите на източване на кредитни и дебитни карти. Загубите на банките тук са свързани не само с финансовата стойност на откраднатa сума, но и с отлив на засегнатите клиенти на банката (Evers, 2012). В глобален план между една трета и една четвърт от потребителите са ставали жертва на картови измами. Причините се крият в това, че при използването на картите на банкомат или ПОС-терминал те лесно могат да бъдат скимирани и след това фалшифицирани. При безналичните транзакции за банките е трудно да удостоверят дали истинският картодържател извършва плащане при онлайн пазаруване в Интернет, или е киберпрестъпник (Парушева, 2005 г., с. 103). Тук не бива да бъде подценяван и рискът от кражба на лични данни и възможността за злоупотреба с тях.
- Банкови бази данни. Голяма част от банките използват SQL сървър, в който се съхранява цялата база данни на всички клонове на банката. SQL сървърът е уязвим от гледна точка на все по-усъвършенстваните "инжекция"-атаки. Пораженията тук могат да се сведат до загуба на данни и изтичане на информацията. Така банките могат да се окажат в несъстоятелност и да се блокират основните бизнес процеси, протичащи в тях. Това би нанесло сериозни финансови и репутационни щети.
- "Гмуркане в боклука". Банките, които не вземат подходящи мерки за унищожаване на информация на хартиен носител, рискуват поверителната им информация да попадне в неподходящи ръце. Същото се отнася и за информация, съхранявана на носители като CD-та и DVD-та, както и печатни материали. При осъществяване на банкови сделки с клиенти хартиени носители задължително се запазват в определен срок. Важно е архивирането и унищожаването на информацията след изтичане на срока да бъде извършено по установени правила.
- Фишинг сайтовете и спам. Онлайн фишингът е начин потребителите на компютри да бъдат измамени така, че да разкрият своя лична или финансова информация в имейл съобщение или уеб сайт. Най-често онлайн фишингът започва с имейл, който изглежда като официално съобщение от надежден източник, например банка или фирма за кредитни карти. Съобщението може да изглежда легитимно и да съдържа запазените знаци на организацията, а имейл адресът да наподобява този

на фирмата, от името на която се изпраща съобщението. В имейла получателите биват насочени към измамнически уеб сайт, където им се поисква да предоставят конфиденциални секретни данни, например име и парола за достъп до интернет банкиране, номер на банкова карта, CVV\CVC или др. След това тази информация може да се използва за кражба на самоличност и последваща финансова измама и щета. За предотвратяване на този риск е важно банковите клиенти да не предоставят конфиденциална информация, свързана с достъп до интернет банкирането или до банкова карта чрез интернет или телефон. Тази информация не е необходима на банката и няма да бъде поискана от клиентите при никакви обстоятелства. Тук е необходимо клиентите да обръщат внимание на адреса на подателя.

- Фарминг. При този метод също се използват фалшиви уеб сайтове, но не се изпращат имейл съобщения. Фармингът се осъществява чрез т.нар. атака "DNS poisoning" или чрез промяна на "hosts" файла в компютъра на жертвата. По този начин се пренасочва трафикът от определен уеб сайт към друг, който е негово копие и има за цел кражбата на секретна информация като потребителско име, парола и др. При "DNS poisoning" DNS сървърът преобразува адресите на уеб сайтовете, които клиентът пише в адресната лента на уеб браузъра, в IP адреси. Например, когато се напише "www.dskdirect.bg", компютърът ще се обърне към DNS сървъра на интернет доставчик, за да научи IP адреса на сайта и да го отвори. Ако той бъде подменен с друг адрес, при изписването на www.dskdirect.bg, заявката ще бъде пренасочена към сървър, съдържащ точно копие на сайта на банката. Потребителят има вероятност да не разбере за измамата, защото е написал собственоръчно адреса на уебсайта. При промяната на "hosts" файла в компютъра на жертвата зловредна програма би могла да модифицира файла и по този начин да бъде откраднатa ценна информация от жертвата.
- Вишинг. Вариант на метода фишинг, при който имейлите съдържат телефонен номер, на който се препоръчва потребителите да се обадят, за да потвърдят потребителските си идентификатори или друга секретна информация. В имейла може да се крие и вирус, чрез който измамникът заразява компютъра на жертвата и получава пълен достъп до данните, включително до банкови сертификати (Препоръки за сигурност в интернет).
- Пре-фишинг. Той се очертава като нов метод, използван от измамници, който се проявява първоначално като разузнавателна атака. Вместо да се опитва директно да получи пълномощия върху данните на банковите клиенти, атаката се стреми да установи потребителските

им имена и комбинации от паролите им. Тук се залага на факта, че потребителите ще използват същите пароли или подобни комбинации за регистрация в различни уеб сайтове. По този начин фишърите могат да се сдобият с информацията, която клиентът ползва за достъп и осъществяване на финансови движения в съответния банков сайт за електронно банкиране.

- Телефонни измами. Някои от най-честите сценарии са свързани с:
  - Телефонни позвънявания до банков служител от телефонен номер, приличащ на вътрешните банкови номера, като ответната страна твърди, че е служител в друг офис и се нуждае от определена банкова информация;
  - Телефонни разговори с нищо неподозиращи служители от страна на злонамереното лице, което с добра аргументация ги подтиква към изпращане на чувствителна информация;

Служители, които не разпознават факта, че информацията е чувствителна, са основни мишени. Фишинг имейли и други подобни измами разчитат на невежество, глупост, наивност, алчност и много други човешки слабости.

- Физическа кражба. Физическата кражба все още си остава рискова зона. Освен банковите офиси, обект на кражба са и преносими компютри, флаш памети и др. Най-често този род кражби се извършват върху лаптопите на мениджърите, когато ги оставят без надзор по време на работни обеди в автомобилите си, на командировки и др.

За търговските банки загубите от изтичане на информация нанасят както сериозни финансови поражения, така и накърняване на репутацията. Загубата на репутация, от своя страна, е сериозна заплаха за съществуването на банката. Даването на публичност за изтичане на банкова информация, независимо дали е умишлено, или не, би дало сериозно отрицателно отражение върху бизнес процесите, протичащи в банката. Именно поради тази причина търговските банки, развиващи дейност на територията на страната, не бива да допускат загуба на информация под каквато и да е била форма.

5. Третиране, превенция и контрол върху риска от изтичане на информация

Какво могат да направят търговските банки, за да предотвратят загуби на информация?

За да се управлява ефективно рискът от загуба на информация, трябва да бъде съставена ясна програма, включваща минимум следните пунктове:

- Третиране на риска от умишленото или неумишленото разкриване на чувствителни данни – в покой, в употреба или в движение, на неоторизирани лица;
- Поддържане на необходимото равнище на сигурност и осигуряване на използваемост на информацията;
- Защита на данните на банковите клиенти и репутацията на банката;
- Защита на личната информация, обработвана в банката;
- Осигуряване на постоянен контрол (Data Loss Prevention keeping your sensitive data out of the public domain, 2011, p. 10)

Започвайки от първия пункт – за защитата на данните при различните състояния на информацията, трябва да се вземат конкретни мерки. Те схематично са показани в табл. 1.

Продължавайки с работата по превенция на изтичането на чувствителна информация, се стига до осигуряване на необходимото ниво на информационна сигурност, което да не нарушава възможността за лесен достъп до информация, необходима за осъществяване на основните бизнес процеси, протичащи в търговските банки. Тук следва да се отбележи, че само по себе си изграждането на добрата информационна система за сигурност не работи във вакуум. Например, ефективно логически контрол на достъпа може да е налице, но ако физическият контрол се провали и чувствителна информация бъде изнесена на хартиен носител, то нейната роля се обезсмисля.

За нуждите на предотвратяване изтичането на информация може да бъде приложен софтуерен продукт, който открива и предотвратява неоторизираното използване и предаване на данни и може да се настрои за идентифициране и осъществяване на мониторинг за защита на данни и употреба на данни в движение и в покой.

Няколко са основните препоръки, които трябва да се следват, за да бъде превенцията срещу изтичане на информация ефективна (DATA BREACH INVESTIGATIONS REPORT, 2014, p. 7), а именно показаните във фигура 5.

Таблица 1. Мерки за третиране на риска от изтичането на информация при различните състояния на данните

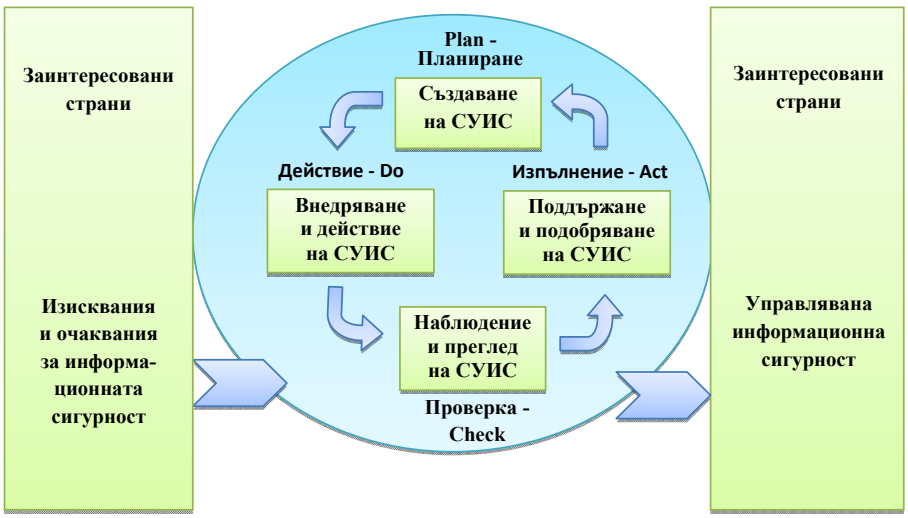
Данни в движение	
Фокус	**Превенция**
Сигурността на периметъра	Предотвратяване изтичането на чувствителни данни от периметъра на банката;
Мониторинг на мрежата	Наблюдение на трафика в мрежата с цел идентификация на трансфера на чувствителни данни;
Контрол на достъпа в интернет	Предотвратяване на достъпа на потребителите до неразрешени сайтове или качване на данни чрез интернет – чрез лична поща, социални мрежи, онлайн инструменти за архивиране и т.н.;
Събиране на информация и обмен с трети страни	Увереност, че обмен на данни с трети страни се извършва само чрез сигурни средства;
Използване на „instant messaging“	Предотвратяване на трансфер на файлове чрез мигновени съобщения и други не-уеб-базирани приложения;
Отдалечен достъп	Увереност в това, че отдалеченият достъп до мрежата на банка е обезпечен;
Данни в употреба	
Мониторинг на определени потребители	Наблюдение върху действията на определен потребител, склонен към заобикаляне на мерките за сигурност;
Мониторинг върху използването на достъп	Наблюдение върху достъпа и използването на високо рискови данни за идентификация на потенциално неправилната им употреба;
Санитарна обработка на данни	Премахване/скриване на определени чувствителни данни, когато те не са необходими за конкретна употреба;
Редукция на тестова информация	Да не се използват или копират чувствителни данни в небанкови системи. Премахване на данни преди да се преместят в тестови системи;
Редакция на данните	Премахване на чувствителните данни от доклади и интерфейси, когато те не са необходими за използването по предназначени;
Експорт/сейф контрол	Ограничаване на потребителските възможности за копиране на чувствителни данни в неодобрени, електронни пощи и уеб-браузъри, включително контролиране на възможността да се копират и печатат части от документи.
Данни в покой	
„Endpoint security“	Ограничаване на административния достъп на банковите служители и елиминиране на възможността за инсталиране на софтуер и променяне на настройките за сигурност. Предотвратяване на зловреден софтуер, вируси, шпионски софтуер и т.н.;
Криптиране	Осигуряване на защита на твърдите дискове на всички сървъри, работни станции, преносими компютри и мобилни устройства;
Мрежово/интернет съхранение	Ограничаване на достъпа до сървърите, съдържащи чувствителни данни;
Изхвърляне или унищожение	Контрол върху цялото оборудване, съхраняващо чувствителни данни, и елиминиране на излишните процеси, които товарят устройствата.

Източник: Data Loss Prevention keeping your sensitive data out of the public domain, Insights on governance risk and compliance, 2011, p. 16-17.

Фигура 5. Стъпки за създаване на ефективна превенция на изтичането на информация

В областта на информационната сигурност е приет и международният стандарт ISO/IEC 27001:2005 за информационни технологии, предлагащ използването на процесния подход при изграждането, внедряването, действието, наблюдението, прегледа, поддръжката и подобрението на системата за управление на информационната сигурност (СУИС). Чрез него може да се осъзнае и необходимостта от създаване на политика и цели на информационната сигурност; внедряването и прилагането на различни начини на контрол в контекста на управлението на риска; наблюдението и прегледа на

действието и ефективността на СУИС; както и непрекъснато подобрение, основано на обективни измервания. Този международен стандарт приема модела "Plan-Do-Check-Act" (PDCA), който се използва за всички процеси в рамките на СУИС.



Фигура 6. Прилагане на PDCA модела към процесите на СУИС

Източник: ISO/IEC 27001:2005

Планиране (създаване на СУИС) – Предполага създаване на политика цели, процеси и процедури на СУИС във връзка с управлението на риска и подобряването на информационната сигурност за постигането на резултати в съответствие с общата политика и цели на организацията.

Действие (внедряване и действие на СУИС) – Внедряване и действие на политиката, контролите, процесите и процедурите на СУИС.

Проверка (наблюдение и преглед на СУИС) – Оценка и, където е приложимо, измерване на изпълнението на процесите спрямо политиката по сигурността, целите и практическия опит и докладване на резултатите пред ръководството за преглед.

Изпълнение (поддържане и подобряване на СУИС) – Предприемане на коригиращи и превантивни действия, базирани на резултатите от прегледа от страна на ръководството, за да се постигне непрекъснато подобряване на СУИС (ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements, p. 4-5).

Частичните дълбочинни интервюта са проведени при срещи с мениджърите по банкова сигурност в изследваните банки. Наред с попълването на анкетните въпроси, те са споделили експертните си виждания и мнения относно тематиката на изследването.

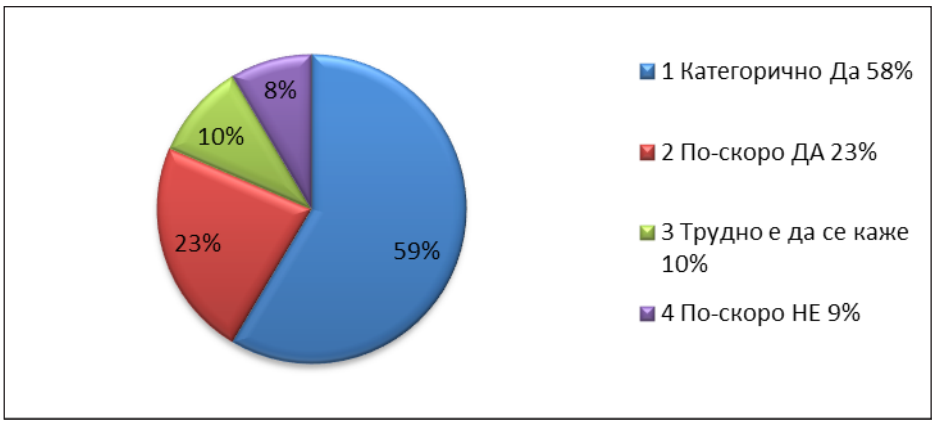
Извадката от изследваните банки включва около 30% от банковия сектор, лицензиран да извършва банкова дейност на територията на България. С цел създаване на по-пълна картина са изследвани различни банки, включително БНБ, Дружеството за касови услуги, което се явява посредник между Централната и търговските банки, Райфайзенбанк – България; Юробанк; Пиреосбанк; Първа инвестиционна банка; Централна кооперативна банка и др.

Моментът, към който е проведено емпиричното проучване, е последното тримесечие на 2015 година. Периодът, който е изследван, е три години. Респондентите са мениджърите по банкова сигурност, към чиито ресор попада информационната сигурност и те съответно са отговорни за превенцията на изтичането на информация от поверените им банки. Използвани са различни статистически методи и средства при обработката на данните от анкетните карти и интервютата.

С емпиричното проучване се цели получаване на достоверна информация по изследваната проблематика, на чиято основа да бъдат извършени необходимите анализи, изводи и обобщения. Това ще бъде предпоставка за извеждане на потенциалния ефект от проявлението на риска, както и тежестта, с която би се проявил той. Предвид деликатния характер на въпросите и запазване конфиденциалността на получената информация, данните се представят в обобщен вид за извадката от банки.

6.2. Резултати от проведеното проучване

Всички запитани мениджъри по банкова сигурност споделят, че дестабилизацията на банковата система от лятото на 2014 г. е дала отражение върху дейността на техните банки. Около 40 % от банките са претърпяли финансови загуби и отлив на клиенти. За други около 40% от тях отражението е било положително, свързано с приток на нови клиенти и парични потоци, подписване на нови корпоративни договори. За 13% от банките дестабилизацията е довела и до сериозни репутационни щети. Неминуемо всичко това се е отразило и върху банковата сигурност. Респондентите споделят, че за кратък период мерките за сигурност са се повишили драстично, което е обострило тяхното внимание. Други от тях са въвели нови мерки за повишаване нивото на сигурността. При трети не се е проявила необходимост от промяна на мерките, свързани с осигуряване на банковата защита.

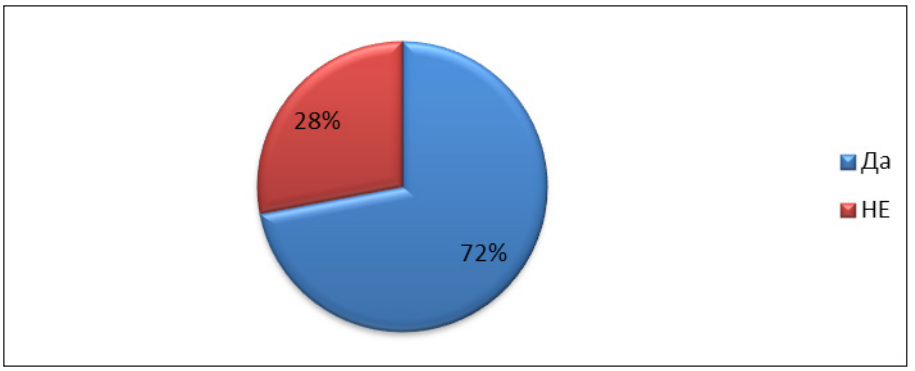


Фигура 7. Отражение на дестабилизацията на банковата система върху банковата сигурност

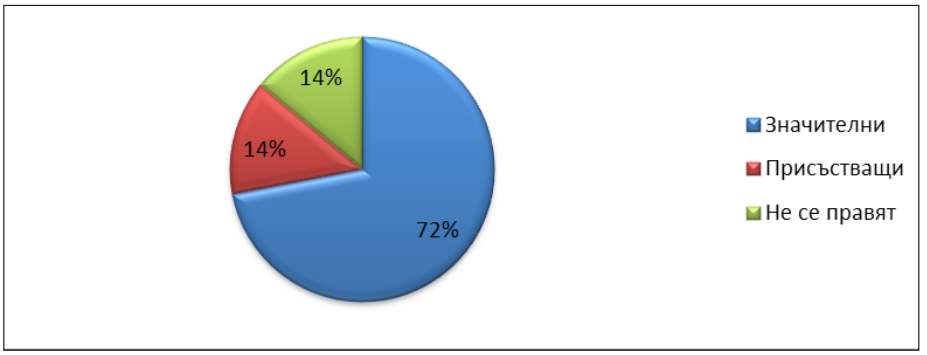
Във връзка със заплахата, свързана с риска от банкови обири, около 65% от мениджърите по сигурността споделят, че според тях през последните три години този риск е намалял. Въпреки това, около 75% заявяват заплаха за сигурността на банковите активи, живота и здравето на персонала. През последните три години 14% от търговските банки са били обект на обири. Основно правило е, че при банковите обири най-често има замесени вътрешни лица. В около 55% от банките е установено, че служителите им са ставали обект на въздействие (подкупи, ухажване, заплахи и др.) от страна на злонамерени лица. В 43% от банките през последните три години банкови служители са правили опити за присвояване или злоупотреба с банкови активи.

Подобен е и процентът на банковите служители, чрез които е изтекла банкова информация. Освен от служители, опити за злоупотреби се наблюдават и от страна на банковите контрагенти. Тук се имат предвид фирми по поддръжката, външни софтуерни специалисти, консултанти, доставчици и др.

По отношение на банковите звена по сигурността мениджърите оценяват квалификацията на служителите, занимаващи се с физическа защита на банковите сгради, като висока (43%) и средна (57%). В 71% от банките се правят инвестиции в поддържането и повишаването на тяхната квалификация. Около 70% от мениджърите намират и отдела си за банкова сигурност като достатъчно надежден и способен да реагира на заплахите на средата.

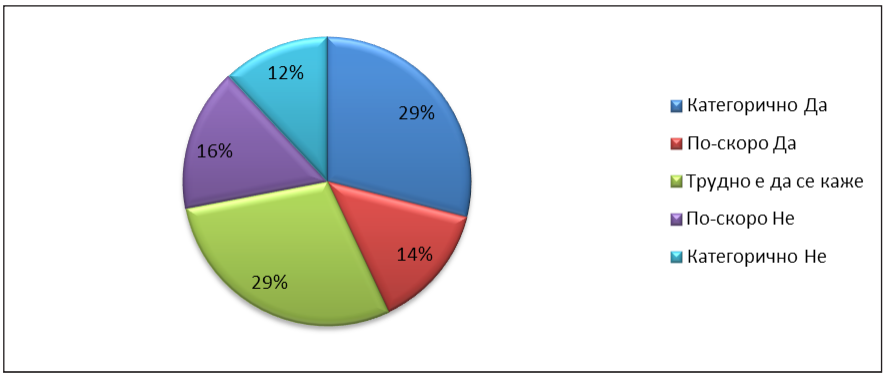


Фигура 8. Наличие на заплаха за сигурността на банковите активи от страна на злонамерени лица



Фигура 9. Наличие на инвестиции в процеса по повишаване на квалификацията на заетите в банковата сигурност

Друга рискова група за банковата сигурност е банковият персонал. През последните три години в 43% от банките мениджърите по сигурността са имали проблеми с надеждността на персонала. Те са установили опити за заобикаляне/ нарушаване на разпоредбите за банкова сигурност от страна на персонала на банката. С цел гарантиране на високо ниво на банкова защита отделите по банкова сигурност са осъществили доверителни отношения с банковия персонал при ежедневни разговори и за изясняване на определени обстоятелства при различни събития (86% от случаите). Друг фактор, определящ надеждността на персонала, е свързан с неговата мотивация. В едва 29% от банките служителите са определени като високо мотивирани. В другата крайност – немотивирани – са 14%.



Фигура 10. Надеждност на банковия персонал

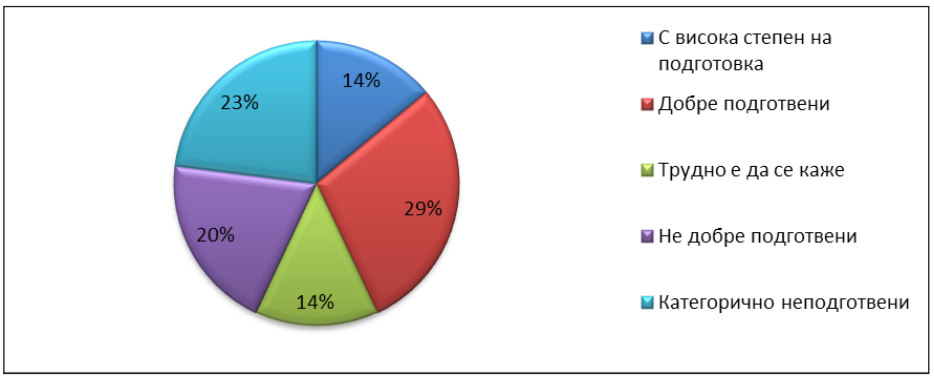
Следващата рискова група, анализирана в настоящия труд, са техническите системи за сигурност. При 86% от банките мениджърите по сигурността смятат, че инвестициите в иновации, свързани със системата за физическа защита, осъществявани при тях, са целесъобразни. Те осигуряват високо ниво на защита или поне не по-ниско от това на конкурентните банки. В голямата си част търговските банки намират за необходимо въвеждането на нов тип технически елементи на системата за физическа защита. Естествено, когато това е продиктувано от измененията в средата и е целесъобразно за конкретния обект, се предлага по-висока степен на защита на банката. 57% от банките виждат необходимост от засилване на мерките за сигурност в отговор на нарасналата заплаха от елиминиране/заглушаване на техническите системи за сигурност от страна на недоброжелатели.

В същото време се работи и в посока за намаляване на риска от елиминиране на незащитени (нерезервирани) технически системи за сигурност. През последните години всички изследвани банки са имали срив (повреда) в някоя от системите за техническа защита. В мнозинството си тези повреди са били малки и оперативно отстраними в рамките на деня. 43% от банките обаче са се сблъскали и със сериозни сривове, които са довели до загуба на информация.

Инкасовият транспорт също подлежи на сериозни анализи, що се отнася до банкова сигурност. Мнението на 30% от мениджърите по сигурността е, че инкасовият транспорт не е достатъчно надежден. Едва 14% от банките го определят като категорично надежден. Този отговор са дали банките, които осъществяват собствен инкасов транспорт. Повечето от големите търговски банки обаче не се занимават с извършването на такъв род дейност, аутсорсват я на специализирани компании с голяма регионална мрежа. По този начин самите банки нямат пряк контрол при преноса на ценните си пратки,

а от тук идват и редица проблеми. Над 70% от мениджърите по банкова сигурност смятат, че рискът от обири върху инкасови автомобили се е увеличил. През последните пет години при транспорт на ценни пратки при 15% от банките е бил извършен грабеж.

Освен това, по експертното мнение на запитаните (43%), инкасовите екипи не са достатъчно подготвени за реакция в случай на заплаха срещу тях. Наблюдава се липса на стриктност при изпълнение на процедурите за транспорт, приемане/предаване на ценни пратки, съобразно изискванията на Наредба I-121 за реда и организацията на охраната при транспорт на ценни пратки и товари. Често нарушение е, че не се спазва изискването относно числеността на екипа, извършва се пренатоварване на ценни пратки между отделни автомобили в незащитени зони и т.н. Банковата практика сочи, че опитите за злоупотреби от страна на инкасовите служители върху поверените им ценни пратки също се повишават.



Фигура 11. Степен на подготовка за реакция на инкасовите екипи срещу заплахи

Втората част от емпиричното изследване обхваща специализиран кръг от въпроси, свързани с изтичането на информация от банките. Мнението на банковите експерти по сигурността е единодушно, че заплаха за сигурността на информацията крият както вътрешните, така и външните източници. Рискови се оказват и преднамерените, и непреднамерените действия на банковите служители. По-голяма степен на заплаха мениджърите виждат в непреднамерените действия на банковите служители, свързани с прескачане на определени мерки за сигурност, невнимание, недоосмисляне, недоразбиране на определени процеси и т.н. През последните три години в около 50% от банките е имало изтичане на информация. Ситуациите, които провокират банковите служители да прибягнат до изнасяне на информация, са твърде

многообразни. По време на проведеното изследване бяха разграничени няколко потенциални хипотези, свързани с изнасянето на информация, които банковите мениджъри оцениха. С цел постигане на единна оценка бе въведена числова скала от едно до пет, като с пет се оценява най-високата степен на риск. Така се достигна до получаване на следните отговори:

Първа хипотеза – при внезапно напускане на служител. Потенциалната опасност в тази ситуация е свързана с планиране на определени действия от служителя и изчакване на подходящ момент за оповестяване на решението. Рисков е периодът между вземането на решение от страна на банковия служител и момента на неговото оповестяване. Тази рискова ситуация – по скалата от едно до пет, банковите мениджъри по сигурност оцениха с 2,9.

Втора хипотеза – при преминаване в конкурентна банка. Потенциалният риск тук се крие в банковия портфейл, с който разполага служителят, и в привличането на неговите клиенти на новото работно място. Друга заплаха е свързана с възможността въпросният служител да разкрие чувствителна информация на новото си работно място. Тази рискова ситуация мениджърите оцениха с 3,3.

Трета хипотеза – когато служител е поставен под зависимост. В този случай съществува потенциалният риск от налагане на определен външен натиск върху такъв банков служител. Тези въздействия най-често се свързват с притискане чрез заплахи, изпадане в несъстоятелност на служителя или негови близки, подкупи, ухажвания и редица други. Банковата практика показва, че тук са и най-честите случаи, при които служители прибягват до злоупотреби и изнасяне на банкова информация. По отношение на оценката на този случай банковите мениджъри по сигурността са единодушни и поставят най-високата оценка за нивото на риск – пет.

Четвърта хипотеза – когато служителят е уволнен. Този случаи е двулик: от една страна, съществува моментът на изненадата, при който банковият служител е информиран за прекратяване на трудовите си правоотношения с банката и всички достъпи до информация му се отнемат на момента. От друга страна, тук е важна реакцията на служителя. Ако той е ядосан и реши да отмъщава, може лесно да нанесе репутационни щети чрез пускане на слухове или да разгласи информация, която му е била известна във връзка със задълженията, които е имал и т.н. Оценката, с която бе оценен експертно този потенциален случай, е 2,9.

Пета хипотеза – когато служителят има лични отношения с журналисти. Пред този потенциален риск също са изложени всички банки. Неговата честота като че ли е най-малка от всички изброени по-горе. Той е оценен и с най-ниската оценка – 2,3.

Фигура 12. Случаи на изнасяне на информация

По време на изследването бе обърнато внимание и на банкови злоупотреби на служители, склонни към изнасяне на информация, свързани с техния пол. Над 80% от отговорите бяха, че полът не е определящ. По-голямата част от служителите в търговските банки са жени, но, от друга страна, преобладават мъже на по-стратегически постове с достъп до банкова и чувствителна информация. Така изследването показа, че разпределяйки пропорционално съотношението жени-мъже и анализирайки случаите на изнасяне на банкова информация, полът не е определящ, а по-скоро индивидуалната нагласа на отделните личности.

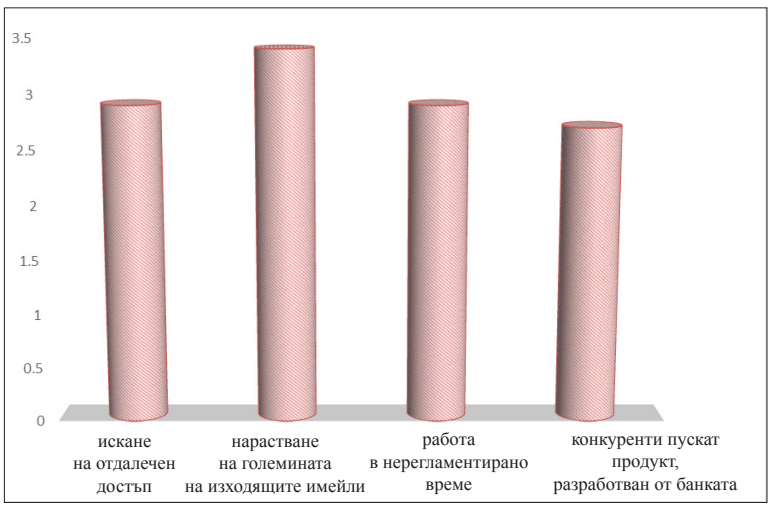
Оценени са и потенциалните ситуации, при които се наблюдават злоупотреби с чувствителна информация. Отново е използвана числова оценка със скала от 1 до 5. Отново 5 е оценката за най-висока степен на риск. Наличието на подобни случаи трябва да алармира за необходимо изостряне на вниманието на служителите по сигурността.

Първи случай: Внезапно искане на отдалечен достъп без основателна причина. В част от банките отдалеченият достъп е забранен, с което те елиминират наличието на подобен риск. В същото време се затруднява комуникацията що се отнася до мениджърското равнище или дейността на информационното обслужване без такъв достъп. Оценката на този риск по възприетата скала е 2,9 пункта.

Втори случай: Внезапно нарастване на големината на имейлите, които изпраща даден служител. Според запитаните респонденти, за този риск от потенциално изтичане на информация оценката и възможността за реализацията му е по-висока – 3,9 пункта.

Трети случай: Работа в нерегламентираното работно време – късно вечер или през почивните дни. В по-голямата част от банките работното време е строго дефинирано и следено със системи за контрол на достъп и отчитане на работното време. Въпреки това, възможности за използване на обедни почивки и други промеждутъци от време винаги могат да бъдат намерени и съответният служител да извърши потенциалното нарушение. Възможността за сбъдване на този риск бе оценена с 2,9 пункта.

Четвърти случай: Ако конкурентна банка необичайно бързо пусне на пазара продукти или услуга, по които се работи в разглежданата банка. Този риск бе оценен с най-ниска оценка поради причината, че в търговските банки продуктите, които се пускат на пазара, са със сходен характер. Оценката за сбъдване на този риск е 2,7 пункта.



Фигура 13. Случаи, сигнализиращи за наличие на злоупотреба

Друга потенциална възможност за изтичане на информация е възможността за използване на приложения от групата "Instant Messaging". На определени работни позиции те биха улеснили комуникацията между банковите служители и клиентите и контрагентите на банката. Едва в около 30% от банките такъв достъп има само на определени позиции, нямащи пряк достъп до банкова информация, като в нито една от банките не е установявано изтичане на информация от такъв достъп. По възприетата скала за оценка на риска, тук мениджърите по сигурност поставиха оценка 3,4 и така оцениха потенциалния риск от изтичане на информация чрез използване на приложения от групата "Instant Messaging".

На следващо място бе оценена възможността за изтичане на информация чрез използването на служебните и личните имейли на служителите. В 14% от банките е установено изтичане на банкова или чувствителна информация чрез изпращане на неоторизирани служебни имейли. Банковите служители по сигурността не са установявали загуба на информация вследствие на погрешно прикачен файл или грешно избран получател при използване на служебните имейли. В около 30% от банките на определени позиции банковите служители имат достъп до личните си електронни пощи. При тяхното използване не са установявани опити за злоупотреби. Рискът от изтичане на информация чрез използване на ел. поща е оценен с 3,9 пункта.

Друга алтернатива за склонните към изнасяне на информация банкови служители е използването на различни блогове и форуми, където – волно или не, коментирайки определени обстоятелства, те публикуват и информация, определяна като чувствителна или дори банкова тайна. През последните 3 години в около 30% от банките са се сблъсквали с подобен проблем.

Сериозна заплаха пред всяка информационна сигурност са външните атаки, свързани с прихващане на зловреден софтуер от страна на оперативната банкова техника. Този род атаки засилват своята мощ и са създали проблемни ситуации в 43% от банките. От тях, в 29% се е стигнало до загуба на информация и нарушаване на нейната цялост. Този риск от загуба на информация по възприетата скала се оценява от запитаните мениджъри по банкова сигурност с 3,1 пункта.

Неминуемо, при осъществяването на ежедневната дейност, в търговските банки се използва FTP (файл трансфер протокол) за пренос на данни между компютри и локалната банкова мрежа. В това направление отново се проявява потенциален риск. Търговските банки у нас обаче не съобщават за установено изтичане на информация в това направление. От тук личи и сериозната работа на служителите по информационна сигурност. Използването на локална мрежа донякъде е намалило атаките от злонамерени въздействия в това направление.

Друг стар и утвърден начин за изнасяне на информация е отпечатването ѝ на хартиен носител. За последните 3 години в банковите звена по сигурност не е установявано такъв род нарушение, въпреки че оценката за неговата потенциална реализация е висока, а именно – 4. На следващо място като подобен род заплаха, която е лесна за реализация, е изнасянето на информация чрез използване на камера на мобилен телефон. 43% от банките са се сблъскали със сбъдването на този риск през последните години. Тук оценката на възможността от сбъдване на този риск е 3,7 пункта.

Друг проблем, с който се сблъсква практиката, е загубата на информация като следствие на неадекватно съхранение на архивни единици. Преди ня-

колко години пресата гръмна с новината, че личните данни на банкови клиенти са се разхвърчали по улицата, близо до контейнери, в които търговска банка изхвърлила архива си. Едва 14% от банките обаче съобщават за изтичане на информация вследствие на неадекватно съхранение и унищожаване на лични данни и банкова информация.

За осъществяване на дейността на определени работни позиции/длъжности в банките неминуемо се налага използването на флаш памети (за счетоводители, за ел. подписи и др.), а респективно и разрешаване на достъп до USB портовете на съответна група от банковите компютри. Така те стават лесна мишена за сбъдване на риска от изтичане на информация чрез използване на флашки и друг вид памети. Над 80% от банките съобщават, че през последните 3 години не са се сблъсквали с реализирането на загуби от подобен род, но стои въпросът за възможността такива случаи да се проявят. Оценката, поставена от експертите за сбъдване на този риск е 3,6 пункта. А продължава да съществува и рискът от загуба на информация чрез чисто физическата загуба или кражба на устройства като флашки и лаптопи. В около 30% от банките през последните години ключов персонал е губил информация в следствие на загубени или откраднати устройства.

Рискът от замаскиране на информация чрез достъп до прокси услугата и кодиране на данните е оценен като възможен с оценка 3,1 пункта, но с такъв проблем към момента банковата практика у нас не се е сблъсквала.

Друг сериозен риск, който печели все по-голяма популярност напоследък, е източването на кредитни и дебитни карти на банкови клиенти. Тук основният проблем се крие в действията на ползвателите на картите. Голяма част от злоупотребите с дебитни карти се основава на факта, че картодържателите съхраняват пластиката и пин кода на едно и също място. Така, ако банков клиент загуби портфейла си или той му бъде откраднат, и не блокира веднага сметките си, то рискът да загуби пари по сметката си е голям. Разбира се, все по-широко навлиза използването на многообразни скимиращи устройства. Друга голяма заплаха е електронното пазаруване в интернет и използването на кредитни карти за разплащане. В около 50% от банките през последните 3 години сметките на клиенти са ставали обект на атака. Клиенти, претърпели пре-фишинг атаки, свързани с получаване на достъп до електронните им акаунти за банкиране и възможни злоупотреби с тях, има в 86% от проучените банки.

Друг обект на потенциална заплаха от страна на злонамерени лица, целящи достъп до информация, е SQL сървъра на банката. Тук се наблюдава силна защитна борба от страна на експертите по информационна сигурност и, респективно – сериозни външни атаки. Около 30% от банките са се сблъскали с такива атаки, довели до загуба на информация през последните

години. Вследствие на този риск всички пострадали са претърпели и прекъсване на основните бизнес процеси, протичащи в поверените им банки. Прекъсванията в голямата си част са били краткосрочни, но въпреки това е имало сериозни щети. При 14% от изследваните банки загубата на информация е осъществена чрез прихващане на IP-то на даден банков компютър.

Установени опити за достъп до банкова информация са правени и чрез телефонни разговори със служителите на банката (в около 30% от търговските банки). Предвид въведените мерки за сигурност от страна на банките, свързани с уточняващи въпроси за банковите данни, тези опити не са били успешни.

От проведеното проучване могат да се направят следните изводи:

- Актуалното състояние на търговските банки у нас към момента бележи тенденция на стабилност и равновесие;
- Равнището на банкова сигурност е високо, като се правят постоянни инвестиции и се вземат мерки за поддържане на сигурността на информацията;
- Предвид получените резултати от проучването, банките не бива да пренебрегват ролята на персонала и неговите моментни състояния, те следва да работят настоятелно за недопускане на изтичането на банкова информация – било то волно, или не.
- Криминогенната група фактори традиционно се запазва на високо равнище, с което се застрашава целостта на банковите активи, като атаките върху банковите клиенти бележат значителни размери. Това би следвало да мотивира банките да работят за засилване на бдителността на клиентите си, давайки им съвети за повишаване на нивото на собствената им сигурност.
- Изправността на техническите системи за сигурност трябва да е под постоянен мониторинг. Нарастват заплахите от пробиване на защитните стени на информационната сигурност с все по-мощни и разнообразни като похвати хакерски атаки.

7. Оценка на ефекта от изтичането на информация и препоръки за неговото управление

Проведеното емпирично проучване – наред с илюстриране на равнището на идентифицирания и анализиран риск, има за цел и да бъде предпоставка за извършване на оценка на ефекта от изтичането на информация от банките. Оценката на риска зависи от честотата на рисковите събития, тяхната сериозност, а също и от тежестта на последствията, които биха причинили. Имайки предвид обобщената честота на проявление на описания риск за изследвания период (3 години), може да се каже, че тя е на средно ниво.

Сериозността на проявлението не е била на критични нива, но е довела до средни по тежест икономически и репутационни вреди за банките, в които се е проявила. На тази основа може да се определи, че оценката на риска, свързан с изтичане на информация от банките, е средна и следва да бъде управлявана. Тази оценка няма за цел да даде количествени характеристики на риска. Това би предизвикало затруднение поради широкия обхват на изследваните данни и необходимостта всеки отделен обект да бъде рисково оценен. Дадената оценка на риска има за цел да накара банковият мениджмънт да се замисли за икономическия ефект от сбъдването на рискови събития от тази група.

Авторовите препоръки за ефективна навременна превенция са свързани в описаните вече мерки за контрол – използване на процесния подход на ISO/IEC 27001:2005 и създаване на специфична за банката система за управление на информационната сигурност, съдържаща планиране, действие, проверка и изпълнение.

Да се създаде подходяща банкова политика и да се разпишат правила относно информационната сигурност: да се класифицират данните според важността им; да се определи достъпът до тях според принципа "необходимо да се знае"; да се обучава регулярно персоналът за работата с информацията и мерките за защита, които служителите трябва да следват; да се поддържа бдителността им на високо ниво; да се поддържа и обновява информационната защита на банката.

Навременната идентификация и превенция на риска от изтичане на информация би спестила значителни средства за възстановяване на загубена или повредена информация; би предпазвала от нарушаване на основните бизнес процеси, протичащи в банките, от отлив на клиенти и сериозни репутационни щети.

ЗАКЛЮЧЕНИЕ

Все по-големият рисков спектър създава все по-големи предизвикателства пред банковите мениджъри. Когато се говори за загуба на данни, превенцията е винаги по-добрата алтернатива пред възстановяването след загуба на банкова информация и уронването на репутацията на банката. С развитието на технологиите значително нарастват и новите заплахи за банковите активи. Загуба на чувствителни данни чрез киберпрестъпността и вътрешните заплахи представлява същността на нарастващите рискове, свързани с прекъсване на основните бизнес процеси в търговските банки. Една банка, която успява да защити информацията си, гарантира запазване на конкурентни

предимства на банковия пазар и осигурява бърза и ефективна реакция при потенциални инциденти.

От проведеното изследване в рамките на настоящия труд се очертаха основните заплахи, пред които са поставени търговските банки. Показана беше честотата на сбъдването им през последните три години. Изводът, който може да бъде направен тук, е, че авторската теза се потвърждава в пълна степен, доказвайки, че всички изследвани банки осъзнават величината на риска от изтичане на информация и работят в направление на неговото адекватно управление. Въпреки редицата мерки за третиране на риска, той остава значим, тъй като нараства и разнообразието от форми на проявлението му. Банковият персонал, с неговите неволни или преднамерени действия, остава сред основните източници на риск, отнасящ се до изтичане на информация. Наред с него, бързото развитие на информационните системи води и до по-значителни и опасни атаки от външни източници. Препоръката, която може да се даде на бизнеса чрез проведеното изследване, е, че превенцията на риска от изтичане на информация се крие преди всичко в постоянен мониторинг на вътрешната и външната среда на банката, в ранна диагностика, анализ и управление на актуалните заплахи.

ЦИТИРАНИ ИЗТОЧНИЦИ:

Димитров, С., 2011. Доклад "Сигурност на информацията и до какво може да доведе бездействието при нейното управление", X регионална конференция по "Информационна сигурност и съхранение на данни", София.
(Dimitrov, S., 2011. Doklad "Sigurnost na informatsiata i do kakvo mozhe da dovede bezdeystvieto pri neynoto upravlenie", X regionalna konferentsia po "Informatsionna sigurnost i sahranenie na danni", Sofia)
Закон за кредитните институции, Обн. ДВ. бр.59 от 21 юли 2006 г., чл. 2; чл. 7-13; чл. 67, 68.
(Zakon za kreditnite institutsii, Obn. DV. br.59 ot 21 yuli 2006 g., chl. 2; chl. 7-13; chl. 67, 68)
Павлов, Г., 2013. Цикъл от лекции по Информационна сигурност, УНСС.
(Pavlov, G., 2013. Tsikal ot lektsii po Informatsionna sigurnost, UNSS)
Парушева, С., 2005. Използване на платежни карти и предотвратяване на измами, свързани с тях, в Европа и у нас, сп. "Икономически и социални алтернативи", УНСС, бр. 4/2005 г., с. 103.
(Parusheva, S., 2005. Izpolzvane na platezhni karti i predotvratyavane na izmami, svarzani s tyah, v Evropa i u nas, sp. "Ikonomicheski i sotsialni alternativi", UNSS, br. 4/2005 g., s. 103)

Препоръки за сигурност в интернет https://dskbank.bg/Page/default.aspx?xml_id=/bg-BG/Individuals/dskdirectpersonal/.security/
(Preporaki za sigurnost v internet https://dskbank.bg/Page/default.aspx?xml_id=/bg-BG/Individuals/dskdirectpersonal/.security/)
Радков, Р., Е. Михайлов, 2002. Банково дело, Свищов, изд. "Деси", с. 35-37.
(Radkov, R., E. Mihaylov, 2002. Bankovo delo, Svishtov, izd. "Desi", s. 35-37)
Семерджиев, Ц., 2004. Информационна сигурност, София, изд. "Софттрейд", с. 24.
(Semerdzhiev, Ts., 2004. Informatsionna sigurnost, Sofia, izd. "Softtreyd", s. 24)
Antony, P., A. Melek, 2010. Data Leak prevention, ISACA, p. 5, 6.
Brunnermeier, M., 2005. Information Leakage and Market Efficiency, Princeton University.
Carvalho,V., W. Cohen, 2012. Preventing Information Leaks in Email, Camogie Mellon University.
DATA BREACH INVESTIGATIONS REPORT, 2014, p. 7.
Data Loss Prevention keeping your sensitive data out of the public domain, Insights on governance risk and compliance, 2011, p. 10; 16-17.
Data Theft, Grand Thornton International LTD, Institute of Chartered Accountants in Ireland, 2009, p. 4, 12.
Evers, J., 2012. Details emerge on credit card breach.
Gordan, P., 2007. Data Leakage – Threats and Mitigation, SANS Institute, p. 5.
Haclee, J., 2011. Ttechnology and ITS Eeffects in CLASSIFIED INFORMATION LEAKS, DUKE UNIVERSITY, DURHAM.
ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements, p. 4-5; 7.
Keeney. M., 2005. Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors. United States Secret Service / CERT.
Parizo, E., 2007. Super Bowl stadium Web site hacked, delivered malware.
Social Dude, информационна сигурност, http://www.socialdude.net/bg
(Social Dude, informatsionna sigurnost, http://www.socialdude.net/bg)

ПРИЛОЖЕНИЕ:

Уважаеми г-н .....,

Тази анкета е един от инструментите на научно изследване, насочено към установяване на актуалното състояние на банковата сигурност и оценка на риска от изтичане на информация в търговските банки, работещи на територията на страната.

За мен като изследовател е ценна практиката и Вашето мнение, защото те ще покажат дали е възможно прилагането в реална обстановка на разработената от мен методика за управление на риска от изтичане на информация.

Ще Ви бъда изключително благодарна, ако подкрепите моя научен труд и попълните предоставената Ви анкета. Поради деликатния характер на въпросите, моля Ви, дайте отговор само на тези, които прецените. Предоставената от Вас информация ще се използва единствено и само за научна цел, като гарантирам, че ще запазя конфиденциалността на предоставените от Вас данни.

Предварително Ви благодаря за оказаното съдействие, като поемам ангажимента да получите екземпляр от обобщения вариант на данните, които могат да бъдат полезни и във Вашето звено за сигурност.

(Моля, маркирайте отговора, който сте избрали!)

1. Смятате ли, че през последните 3 години рискът от банкови обири се е повишил?	Категорично да По-скоро да, отколкото не Трудно е да се каже По-скоро не, отколкото да Категорично не
2. Дестабилизацията в банковата система от лятото на 2014 г. даде ли отражение в дейността на Вашата банка?	Категорично да По-скоро да, отколкото не Трудно е да се каже По-скоро не, отколкото да Категорично не
3. Вашата банка претърпя ли финансови загуби и отлив на клиенти в следствие на дестабилизираната банкова система?	Категорично да По-скоро да, отколкото не Трудно е да се каже По-скоро не, отколкото да Категорично не

4. Вашата банка претърпя ли репутационни загуби в следствие на дестабилизираната банкова система?	Категорично да По-скоро да, отколкото не Трудно е да се каже По-скоро не, отколкото да Категорично не
5. Дестабилизацията в банковата система даде ли отражение върху банковата система за сигурност?	Категорично да По-скоро да, отколкото не Трудно е да се каже По-скоро не, отколкото да Категорично не
6. Чувствате ли заплаха за сигурността на банковите активи, живота и здравето на персонала, от страна на недобронамерени лица?	Категорично да По-скоро да, отколкото не Трудно е да се каже По-скоро не, отколкото да Категорично не
7. През последните 3 години имало ли е опит за грабеж във Вашата банка?	ДА НЕ
8. През последните 3 години имало ли е реализиран обир във Вашата банка?	ДА НЕ
9. Ваши служители ставали ли са обект на въздействие (подкупи, ухажване, заплахи и др.) от страна на злонамерени лица?	Категорично да По-скоро да, отколкото не Трудно е да се каже По-скоро не, отколкото да Категорично не
10. През последните 3 години имало ли е реализиран опит за присвояване или злоупотреба от служители във Вашата банка?	ДА НЕ
11. През последните 3 години установявали ли сте изтичане на банкова информация от банковите Ви служители?	ДА НЕ
12. През последните 5 години забелязвали ли сте опити за злоупотреби от страна на Ваши контрагенти (фирми по поддръжка, софтуерни специалисти, доставчици на консумативи, консултанти и др.)?	ДА НЕ
13. Как оценявате квалификацията на служителите, занимаващи се с физическата защита на банковите ви сгради?	На високо ниво На средно ниво На ниско ниво

14. Вашата банка инвестира ли в поддържане и повишаване на квалификацията на заетите с банкова сигурност?	Категорично да По-скоро да, отколкото не Трудно е да се каже По-скоро не, отколкото да Категорично не
15. Намирате ли Вашия отдел за банкова сигурност за достатъчно надежден и способен да реагира на заплахите на средата?	Категорично да По-скоро да, отколкото не Трудно е да се каже По-скоро не, отколкото да Категорично не
16. Намирате ли банковия персонал за достатъчно надежден?	Категорично да По-скоро да, отколкото не Трудно е да се каже По-скоро не, отколкото да Категорично Не
17. Установявали ли сте опити за заобикаляне/нарушение на разпоредбите за банкова сигурност от страна на персонала на банката?	Категорично да По-скоро да, отколкото не Трудно е да се каже По-скоро не, отколкото да Категорично Не
18. Осъществявате ли доверителни отношения с банковия персонал?	Когато се наложи за изясняване на определени обстоятелства; При ежедневни разговори; Служителите комуникират само с преките си ръководители
19. Намирате ли банковите служители за достатъчно мотивирани?	Високо мотивирани Добре мотивирани Задоволително мотивирани Не мотивирани
20. Смятате ли, че инвестициите в технически иновации, свързани със СФЗ, осъществени във Вашата банка, са целесъобразни?	Категорично да По-скоро да, отколкото не Трудно е да се каже По-скоро не, отколкото да Категорично не
21. Смятате ли, че техническите системи в СФЗ осигуряват високо ниво на защита, не по-ниско от това в конкурентните банки?	Категорично да По-скоро да, отколкото не Трудно е да се каже По-скоро не, отколкото да Категорично не

22. Намирате ли за необходимо да въведете нов тип технически елементи на СФЗ?	Категорично да По-скоро да, отколкото не Трудно е да се каже По-скоро не, отколкото да Категорично не
23. Необходимо ли е засилване на мерките за сигурност в отговор на нарасналата заплаха от елиминиране/заглушаване на техническите системи за сигурност от недоброжелатели?	Категорично да По-скоро да, отколкото не Трудно е да се каже По-скоро не, отколкото да Категорично не
24. Според Вас високо ли е нивото на риска от елиминиране на незащитени (нерезервирани) технически системи за сигурност?	Категорично да По-скоро да, отколкото не Трудно е да се каже По-скоро не, отколкото да Категорично не
25. През последните 5 години имали ли сте срив (повреда) в някоя от системите за техническа защита?	ДА НЕ
26. През последните 5 години случвало ли Ви се е да загубите информация в следствие на нарушение в работата на някоя техническа система за сигурност?	ДА НЕ
27. Намирате ли инкасовия транспорт за достатъчно надежден?	Категорично да По-скоро да, отколкото не Трудно е да се каже По-скоро не, отколкото да Категорично не
28. Мислите ли, че през последните 5 години рискът от обири на инкасови автомобили се е увеличил?	Категорично да По-скоро да, отколкото не Трудно е да се каже По-скоро не, отколкото да Категорично не
29. Случвало ли Ви се е през последните 5 години при транспорт на Ваши ценни пратки (ЦП) да бъде направен опит за грабеж?	ДА НЕ
30. Смятате ли, че инкасовите екипи са достатъчно подготвени за реакция в случай на заплаха срещу тях?	Категорично да По-скоро да, отколкото не Трудно е да се каже По-скоро не, отколкото да Категорично не

31. Смятате ли, че инкасовите екипи изпълняват стриктно процедурите за транспорт, приемане/предаване на ЦП, съобразени с изискванията на Наредба I-121 от 2004 г., за реда за организиране на охраната при транспортиране на ценни пратки и товари?	Категорично да По-скоро да, отколкото не Трудно е да се каже По-скоро не, отколкото да Категорично не
32. Заплаха за сигурността на информацията във Вашата банка са по-скоро:	Вътрешни източници Външни източници И двата вида
33. В кои действия на банковите служители виждате по-голяма заплаха от изтичането на информация?	В преднамерените действия; В непреднамерените действия; И двете
34. През последните 3 години случвало ли се е във Вашата банка да има изтичане на информация?	ДА Не Трудно е да се каже
35. Как ще оцените изброените случаи на потенциален риск от изнасянето на информация от служител? Оценете отговорите със скала от 1 до 5 като 5 е най- високият риск!	Внезапно напускане на служител; Заминаване в конкурентна банка; Когато служителят е поставен под зависимост; Уволнен служител; Служител, имащ лични отношения с журналисти
36. Според Вас кой от двата пола е по-рисков при изнасянето на информация?	Мъже Жени Полът не е определящ
37. Оценете потенциална злоупотреба на чувствителна информация при следните случаи? Оценете отговорите със скала от 1 до 5, като 5 е най- високият риск!	Внезапно искане на отдалечен достъп без основателна причина; Внезапно нарастване на големината на имейлите, които изпраща служител; Работа в нерегламентираното работно време, късно вечер или през почивните дни; Ако конкурентни банки необичайно бързо пуснат на пазара продукти или услуги, по които се работи в банката

38. На определени работни позиции във Вашата банка разрешава ли се достъп до приложения от групата "Instant Messaging"?	ДА НЕ
38.1. Ако отговорът Ви е "ДА", установявали ли сте опити за изтичане на информация при употребата им?	ДА НЕ
39. Как оценявате риска от изтичане на информация, чрез използване на "Instant Messaging"? Оценете отговорите със скала от 1 до 5 като 5 е най- високият риск!	
40. Установявали ли сте изтичане на информация чрез изпращане на неоторизирани служебни имейли?	ДА НЕ
41. Установявали ли сте изтичане на информация от погрешно прикачен файл или грешно избран получател при използване на служебните имейли?	ДА НЕ
42. Във Вашата банка служителите имат ли достъп до личните си ел. пощи?	Да Не На определени позиции
42.1. Ако ДА, установявали ли сте изтичане на информация чрез използване на лични ел. пощи?	ДА НЕ
43. Как оценявате риска от изтичане на информация чрез използване на ел. поща? Използвайте скалата от 1 до 5!	
44. Установявали ли сте изтичане на информация чрез публикации в различни блогове?	ДА НЕ
45. Случвало ли се е банкови компютри да бъдат заразени със зловреден софтуер?	ДА НЕ
45.1. Ако ДА, претърпявали ли сте загуба на информация вследствие на заразяване на банков компютър със зловреден софтуер?	ДА НЕ

46. Как оценявате риска от изтичане на информация чрез заразяване на банкови компютри? Използвайте скалата от 1 до 5!	
47. Във Вашата банка използвате ли FTP (файл трансфер протокол) за пренос на данни между компютри и локална мрежа?	ДА НЕ
47.1. Ако използвате, установявали ли сте загуба на информация при неговата експлоатация?	ДА НЕ
48. Установявали ли сте изтичане на информация чрез изнасяне на хартиени носители?	ДА НЕ
49. Как оценявате риска от изтичане на информация чрез изнасяне на хартиен носител? Използвайте скалата от 1 до 5!	
50. Установявали ли сте изтичане на информация от снимки, направени с телефоните на служителите?	ДА НЕ
51. Как оценявате риска от изтичане на информация чрез снимки, направени с телефоните на служителите? Използвайте скалата от 1 до 5!	
52. Установявали ли сте загуба на информация вследствие на неадекватно съхранение на архивни единици?	ДА НЕ
53. Разрешено ли е ползването на USB портовете във Вашата банка?	Да Не На определени позиции
54. Установявали ли сте изтичане на информация в следствие използването на устройства като флашки и др. видове памети?	ДА НЕ

55. Как оценявате риска от изтичане на информация чрез използване на флашки? Използвайте скалата от 1 до 5!	
56. Как оценявате риска от замаскиране на информация чрез достъп до прокси услугата и кодиране на данните? Използвайте скалата от 1 до 5!.	
57. През последните 5 години имали ли сте случай на източване на кредитни и дебитни карти на Ваши клиенти?	ДА НЕ
58. През последните 5 години имали ли сте случай на изтичане на лични данни на Ваши клиенти?	ДА НЕ
59. Претърпявали ли сте загуба на информация в следствие на атаки върху SQL сървъра на банката?	ДА НЕ
60. Преустановявали ли сте основните бизнес процеси, протичащи в банката, в следствие на сривове на SQL сървъра на банката?	ДА НЕ
61. Установявали ли сте изтичане на информация вследствие на неунищожени хартиени носители с банкова и/или чувствителна информация?	ДА НЕ
62. Претърпявали ли сте последствия от прихващането на IP-то на банков компютър вследствие от посещение на фишинг сайтове?	ДА НЕ
63. Знаете ли за Ваши клиенти, претърпели пре-фишинг атаки, свързани с получаване на достъп до електронните им акаунти за банкиране и злоупотреби в тях?	ДА НЕ
64. Ваши служители ставали ли са обект на телефонни измами, свързани с достъп до банкова информация?	ДА НЕ Не зная
65. Устройства (лаптопи, флашки и др.п.) на Ваши служители ставали ли са обект на физическа кражба?	ДА НЕ

ПРЕВЕНЦИЯ НА РИСКА ОТ ИЗТИЧАНЕ НА ИНФОРМАЦИЯ ОТ ТЪРГОВСКИТЕ БАНКИ

Резюме:

Информацията е един от ключовите активи на търговските банки. Загубата на банкова информация би нанесла сериозни финансови и репутационни щети за банката. През последните години, при престъпните действия, свързани с банкови обири, все по-често навлизат нови рискове от групата криминогенни рискове. Основно място сред тях заемат киберпрестъпленията, свързани с източване на банкова информация. Настоящата студия е насочена към разкриване на теоретични и емпирични аспекти на превенцията и контрола върху риска от изтичане на информация. Разработена е методична схема за превенция на споменатият риск. Идентифицирани са каналите за изтичане на информация и техният характер. Студията е онагледена с емпирично проучване върху извадка от търговски банки, работещи в България, като е изследвано проявлението на риска от изтичане на информация. Показани са защитните механизми и най-често проявяващите се рискови ситуации, които застрашават банковата информационна сигурност. Очертана е тенденцията по отношение на рисковете при основните вътрешни и външни източници на заплаха.

Ключови думи: търговски банки, банкова сигурност, изтичане на информация, превенция на риска.

JEL: E58; H55; G29.

RISK PREVENTION OF DATA LEAKAGE BY COMMERCIAL BANKS

Abstract:

Information is one of the key assets of commercial banks. The loss of bank information in question might be in serious financial and reputational damage to the bank. In recent years, criminal activities related to bank robberies have been occurring increasingly, bringing new risks of the criminogenic kind. Primary position among them occupy cybercrime connected to drawing off bank information. This study is aimed at revealing the theoretical and empirical aspects of prevention and control of the risk of data leaks. It has developed a methodical scheme for prevention of that risk. Channels of data leaks and their character are identified. The paper is illustrated with an empirical study on a sample of commercial banks, which has studied the manifestation of the risk of leaks. Listed below are the defense mechanisms and most often risk situations that threaten the banking information security. The trend in respect to the risks of major internal and external sources of threat is contoured.

Key words: commercial banks, bank security, data leaks, bank information, risk prevention.

JEL: E58, H55, G29.