Innovations in the Security of Banking Operations

Yordanka Peycheva
University of Economics - Varna, Varna, Bulgaria
yordankapeycheva@ue-varna.bg

Abstract

The contemporary changing technological environment forces all economic units to go through a digital transformation. The banking industry is in the epicenter of this change. Credit institutions seek to adapt a business model that is increasingly customer-oriented, providing new services with greater transparency and levels of security. The growing demand for more effective protection against fraud, phishing attacks, theft of identities and ensuring better levels of security in a timely manner is increasingly central topic in retail banking. The issue of security, as in the territory of bank branches, ATM-devices, as well as in the provision of online and mobile services, arouses the interest of credit institutions to the use of biometric identification technology. Biometric technologies are becoming an indispensable part of the means of personal verification and secure identification activities in banking institutions.

Keywords: digital transformation, banking industry, security, biometric identification

JEL Code: O310

DOI: 10.56065/IJUSV-ESS/2023.12.3.138

Въведение

Технологичният „бум“ провокира вродената иновационна инертност на кредитните институции като отвори нови хоризонти пред осъществяването на банковия бизнес. Бързият растеж на информационните технологии допринесе значително за напредъка на дигиталното банкиране и прогресивно трансформира ежедневни клиентски дейности, обвързвайки ги все повече с цифровото изживяване.

Възможностите предоставени от дигиталното банкиране, донесоха след себе си не само предимства, но поставиха кредитните институции на изпитание пред предизвикателствата на съвременната динамична и несигурна виртуална реалност. Стремежът към минимизиране на човешкия фактор и автоматизиране на всички процеси предизвика, както нови нива на иновационна готовност у банките, така и потенциални пробиви в сигурността ѝ.

Киберпрестъпниците превръщат трезорите в своя основна мишена, насочвайки все повече усилия в търсене на нови начини за посегателства, както спрямо вътрешните системи, така и посредством кражба на лични данни и чувствителната информация за банковите клиенти. Хакерските атаки често използват пропуските в традиционните подходи за сигурност, като липса на споделена интелигентност между изолираните инструменти за безопасност, недостатъчна автоматизация при управлението на рисковете за сигурността и способност за справяне със заплахите в реално време. Разнообразието от вредоносни техники за пробиви в сигурността на банковите институции, като – фишинг атаки, социално инженерство, скимери, ransomware, spoofing и др. предизвикват банките да отговорят с адекватни мерки за защита.

Слабостите на конвенционалните методи за протекция, посредством еднофакторна идентификация (SFA), чрез използването на пароли или PIN кодове се оказват недостатъчно ефективни срещу набезите на киберпрестъпниците. Подобряването на мерките за сигурност, предполага все по-интензивното внедряване на иновативни техники съвместяващи два или повече идентификационен фактор – двуфакторна (2FA) и многофакторна идентификация (MFA).

1. Съвременни заплахи и предизвикателства пред банковия сектор

Финансовият сектор съдържа изобилие от чувствителни данни, които привличат редица заплахи в търсене на бързи печалби. Киберзаплахите могат да окажат значително въздействие върху банковия и финансовия сектор поради поверителността на финансовата информация, създавайки рискове за стабилността, сигурността и целостта на тези институции.

Последните години се оказват благоприятни за покачване нивата на киберпрестъпленията във финансовия свят. Според проучване на Boston Consulting Group от 2019 г., финансовите компании са подложени на кибератаки 300 пъти повече от всички други индустрии – подчертавайки колко привлекателен е този сектор за киберпрестъпниците (Boston Consulting Group, 2019).

Разнообразието от кибератаки във финансовият сектор е завидно – фишинг атаки, социално инженерство, ransomware, различните видове spoofing атаки и др.

Фишинг атаките остават една от най-вредоносните заплахи в банковия сектор и са любим инструмент за кибератаки в съвременния дигитален свят. Киберпрестъпниците използват прикрити имейли или домейни, за да подмамят потребителите да изтеглят злонамерен софтуер или да предоставят лична информация, което иначе е известно като фишинг на идентификационни данни. Изложени на риск от фишинг в банковата индустрия са както клиентите, така и служителите на кредитните институции. Нападателите могат да изпращат имейли, маскирани като официална банкова кореспонденция до клиенти, което може да се окаже ефективно за кражба на финансова информация. По същия начин служителите трябва да бъдат нащрек за подобен вид кибератака, която търси идентификационни данни за вход за достъп до чувствителна информация за клиента.

Според проучване от 2022 г. (CSI, 2022) повечето банкери разглеждат насочените към служителите фишинг атаки като най-голямата заплаха за киберсигурността, като фишингът към клиентите отстъпва с 6% в негативната класация. Резултатите разкриват, че 57% от банкерите са най-загрижени за фишинг, който допуска кибернападателите във вътрешните системи на кредитните институции. Безпокойството на банкерите се дължи на все по-агресивния подход на киберпрестъпниците да подобряват тактиката си за домогване към богатите на данни финансови институции. Според Eurofins фишингът, насочен към служители, бележи ръст след ковид пандемията поради разширяването на дистанционната работа и увеличеното работно натоварване (Eufofins, 2022).

Що се отнася до фишингът насочен към клиентите, 51% от банкерите са загрижени за социалното инженерство, насочено към потребителите чрез фишинг. Киберпрестъпниците продължават да предприемат атаки за имитиране на имейли, представяйки се за обслужващата банка на потребителя, с цел подмамване на клиента за предоставяне на чувствителна информация за акаунта му.

Някои (Airehrour el al., 2018) отличават социалното инженерство като една от най-опасните кибератаки, отчитайки психологическия аспект на вредоносните действия от страна на киберпрестъпниците. От своя страна социално инженерство е злонамерен акт на подвеждане на човек да извърши действие, като обърква емоциите и процеса на вземане на решения. Социалното инженерство е нетехническа стратегия, използвана от кибернападателите, която разчита до голяма степен на човешкото взаимодействие и често включва подвеждане на хората да нарушат стандартните практики за сигурност. Социалното инженерство се различава от традиционното хакване поради обстоятелството, че атаките чрез него могат да бъдат нетехнически и не включват непременно компрометиране или експлоатация на софтуер или системи. Когато са успешни, много атаки чрез социално инженерство позволяват на нападателите да получат законен, разрешен достъп до поверителна информация (Digital Guardian, 2018). Тук на преден план излизат психологическите дименсии за пробив на киберсигурността. Според Digital Guardian,

„атаките чрез социално инженерство обикновено включват някаква форма на психологическа манипулация, заблуждавайки иначе нищо неподозиращи потребители или служители да предадат поверителни или чувствителни данни. Обикновено социалното инженерство включва имейл или друга комуникация, която предизвиква неотложност, страх или подобни емоции в жертвата, карайки я да разкрие чувствителна информация, да кликне върху злонамерена връзка или да отвори злонамерен файл." (Digital Guardian, 2023)

Рансомуеар (*ransomware*) представлява актуален проблем за специалистите по киберсигурност във финансовата индустрия, причинявайки значителни щети на институциите. Тъй като заплахите за киберсигурността продължават да се развиват, рансъмуерът бързо се превръща в заплаха номер едно. За разлика от злонамерения софтуер, който позволява на киберпрестъпниците да крадат чувствителна информация и да я използват на дигиталния пазар, рансъмуерът директно се насочва към собствениците на данни, като държи техните компютърни файлове като заложници, докато не бъде платен откуп (Deloitte, 2016).

Според доклад на TrendMicro само през първата половина на 2021 г. атаките с ransomware в банковата индустрия са се увеличили с колосалните 1318%, което е непропорционално спрямо други индустрии (TrendMicro, 2021). По данни на Sophos процентът на атаките с ransomware във финансовите услуги продължава да бележи ръст от 55% през 2022 г. на 64% през 2023 г., което е почти два пъти повече от 34%, отчетени през 2021 г. Като само 1 от 10 атаки е била спряна преди криптирането, което прави общо 81% от организациите жертва на криптиране на данни (Sophos, 2023).

Spoofing е нов вид кибер заплаха, при който хакерите намират начин да се представят за URL адрес на банков уебсайт с друг такъв, който изглежда и функционира по абсолютно същия начин. Когато потребителят въведе своята информация за вход, тази информация бива обект на кражба от киберпрестъпниците, за да бъде използвана по-късно. По този начин за кибернападателите се възползват от първоначалната заблудата на потребителите и последващото разкриване на финансова и лична информация (Sekhar el al., 2022).

Spoofing атаките се осъществяват в много и различни форми, всички от които включват някакъв вид фалшиво представяне на информация. По-известни сред тях са:

- *Email Spoofing* - Тази техника е една от най-често срещаните, при които киберпрестъпниците изпращат имейл, представяйки се за доверен източник. Те обикновено искат спешна заявка или се опитват да примамят целта да кликне върху злонамерена връзка или прикачен файл (Adlumin, 2023).
- *IP Spoofing* – Това е техника, използвана за получаване на неоторизиран достъп до компютри, при която нарушителят изпраща съобщения до компютър с IP адрес, който показва, че съобщението идва от доверен хост. IP Spoofing може да се използва за скриване на самоличността на кибернападателя, за представяне на друга изчислителна система или и за двете. Обикновено се използва при атаки за отказ на услуга, където целта е да се консумират мрежови ресурси, така че да са недостъпни за предназначените потребители. (DevX, 2023).
- *Caller ID spoofing* - Подобно на подправянето на имейл, Caller ID spoofing е зловредно обстоятелство, при което някой умишлено променя информацията, предадена на дисплея с идентификация на обаждащия се, за да скрие своята самоличност или да се представи за някой друг с цел извличане на лична, чувствителна информация (DevX, 2023). Например, киберпрестъпниците могат да се представят на клиента за представител на обслужващата му банка и да се опитат да съберат лична информация като банкови идентификационни данни, социалноосигурителен номер и т.н.
- *Text message spoofing* - Подправянето на текстови съобщения е техника чрез която киберпрестъпниците подменят определено текстово съобщение, представящи се за доверен източник като обслужваща банка, например. Те заменят идентификатора на

подателя с разпознаваем източник и използват текстовото съобщение като трамплин за кражба на данни, фишинг и измами.

- Facial Spoofing - Разпознаването на лица е в основата на множество системи за удостоверяване в днешно време и бързо разширява своя обхват. Този сравнително нов тип spoofing позволява на киберпрестъпниците да използват уязвимости в технологията, изискваща разпознаване на лица за отключване на устройство или приложение (Adlumin, 2023).

Следва да се отчете обаче и обстоятелството, че революцията в развитието на платежните системи провокира и немалко проблемни моменти, свързани с липсата на унифицирани стандарти. Така например използвания в различните мобилни и уеб приложения приложно-програмни интерфейси (Application programming interface, API) са подложени на потенциални операционни и технологични рискове, а също така могат да породят и ситуации на регулаторно несъответствие, особено при използването от страна на банковите институции. По същия начин опасения за сигурността на данните възникват и по отношение на облачните технологии, свързани с децентрализирано съхранение и обработка на данни (Rafailov el al., 2020).

2. Иновационни техники за осигуряване на сигурност в банкирането – обективна необходимост в съвременната реалност

Еволюцията на цифровите плащания промени начина на управлявление на финансите, предизвиквайки нови изисквания за повишена сигурност. Въпросът със сигурността, както на територията на банковите клонове, АТМ-устройствата, така и при предоставянето на онлайн и мобилни услуги предизвиква интереса на кредитните институции към използването на иновативни техники и технологии за защита на личните данни. Едни от най-важните техники за протекция са тези свързани с процеса по удостоверяване. Методите на удостоверяване постепенно еволюират и усложняват идентификационния процес на субекта.

Еднофакторното удостоверяване (Single-factor authentication (SFA)) е традиционен метод за осигуряване на сигурност, който изисква потребителят да предостави само един фактор на защита, за да получи достъп до онлайн ресурси. Примери в тази насока са използването на парола (или PIN) за потвърждаване на собствеността върху потребителския идентификатор. Тази форма на удостоверяване може да се определи като най-опростената и най-често срещаната, но и най-малко сигурната, тъй като изисква само един фактор за проверка

Като интуитивна стъпка напред в подобряване защитата на личните данни е наложена *двуфакторната автентификация (Two-factor authentication (2FA)). Двуфакторното удостоверяване* е система за сигурност, която изисква две различни форми на идентификация, за получаване на достъп до онлайн акаунт. Този тип удостоверяване съчетава нещо, което знаете (като потребителско име и парола) с нещо, което имате (като приложение за удостоверяване или физически токен) (Ometov et al., 2018).

Токенът за удостоверяване е техника за двуфакторна автентификация. Най-широко рапространеният софтуерен токен е еднократна софтуерно генерирана парола (Acharya, et al.,2013). *Токенът за еднократна парола* е код под формата на парола, поискана в конкретна или произволна ситуация, генерирана от приложението и препратена към регистрирано устройство на потребителя. Операцията се удостоверява, ако паролата е въведена според изискванията в рамките на предварително зададения интервал от време. Тази мярка прави уловените данни за удостоверяване от измамници безполезни за бъдещи атаки следователно паролата се променя динамично и се използва веднъж в рамките на допустимия период от време.

Многофакторните методи за удостоверяване (Multi-Factor Authentication (MFA)) са техники за осигуряване на по-високо ниво на безопасност, улеснявайки непрекъснатата защита на компютърните устройства, както и други критични услуги от неоторизиран достъп чрез използване на повече от две категории идентификационни данни. В по-голямата си част MFA се основава на биометрични данни, което е автоматизирано разпознаване на индивиди въз основа на техните поведенчески и биологични характеристики (Ometov et al., 2018).

Методите на биологичната идентификация най-често включват – пръстови отпечатъци, лицево и гласово разпознаване, сканиране на ириса, както и поведенческа биометрия.

Пръстовите отпечатъци са най-често срещаният метод на избор за банкови биометрични данни поради бързината, лекота на използване, висока точност и рентабилен характер. Институциите за финансови услуги използват пръстови отпечатъци и биометрични данни за пръстови вени в банкирането за идентификация на клиенти в своите филиали, тъй като тези два биометрични метода за удостоверяване дават бързи резултати, които са подходящи за най-натоварените банкови клонове. Освен това, системите за пръстови отпечатъци и пръстови вени са лесни за използване, и гарантират надеждна сигурност. Когато клиентите посещават филиалите на банката, те могат да бъдат удостоверени на гишето чрез пръстови отпечатъци и биометрични скенери за пръстови вени, които съответстват на съществуващия биометричен шаблон на клиента в банковата база данни. След успешно удостоверяване на клиента, същият ще има позволение да продължи напред с банковите си транзакции (Venkatraman, 2008). Идентификацията чрез вените на пръстите се използва най-вече при операции с банкомати. Клиентите поставят един пръст, който е изложен на близка инфрачервена светлина, способна да анализира уникалната конфигурация на вените на индивида. За финансови операции, провеждани както онлайн, така и офлайн, разпознаването на вените на дланта може да служи като цифров подпис, ефективно заместваики други средства за оторизация. През 2014 г. Полша е първата страна в Европа, която въведе разпознаване на вени на пръста на 2000 банкомата в банкови клонове и супермаркети (The Guartian, 2014).

Лицевото разпознаване е базиран на технологии метод за идентифициране на лицето на човек чрез анализиране на лицевите му черти.

Обикновено банките извличат тази информация от снимка или видео. След това тези данни се сравняват с база данни от събрани лица, за да се намери съвпадащ индивид. Софтуерът за разпознаване на лица използва технология, задвижвана от изкуствен интелект (AI). Често банките използват технология за лицево разпознаване за своите процеси за проверка на самоличността. Софтуерът получава видео или изображение с лице на човек. Той сканира тези данни, за да създаде подробна карта на лицевите характеристиките, включително точна информация за очите и други отличителни черти, като белези, например. Въз основа на това сравнение системата за лицево разпознаване определя дали лицевата карта съвпада със субекти от нейната база данни. Въпреки че точността на системата за лицево разпознаване като биометрична технология е по-ниска от разпознаването на ириса и на пръстови отпечатъци, тя е широко разпространена поради своя безконтактен и неинвазивен процес (Petrescu, 2019).

Гласовата биометрия е технологично решение, което позволява автентификация на индивид чрез разпознаване на гласови характеристики и говорни модели. Това е възможно поради уникалността на фонетичните и морфологичните характеристики на гласовия апарат. За да използва гласовата биометрия, компания, прилагаща тази технология, трябва да извърши еднократен процес на записване, включващ извличане на уникален гласов отпечатък от всеки потребител. В случай на пасивна гласова биометрия, записването може да се извърши безпроблемно по време на обикновен разговор, а гласов отпечатък, извлечен от речта на потребителя, се съхранява сигурно в код. Всеки път, когато някой се свърже с кол

център или използва гласа си, докато взаимодейства с приложение или устройство, системата сравнява гласа на клиента със съхранения гласов отпечатък, за да потвърди самоличността му. При използване на такъв тип биометрия, потребителите не трябва да помнят парола или ПИН код, например, защото те се удостоверяват въз основа на чертите и моделите на техния глас (Phonexia, 2021).

Биометричното сканиране на ириса е известен метод за проверка на самоличността, използван за идентифициране на лица въз основа на отличителните модели в техните ириси. Той е признат за своята надеждност, точност и абсолютна сигурност. Традиционните системи за удостоверяване, които разчитат на пароли, пинове и други методи, базирани на знания, могат да бъдат уязвими за хакване за сметка на това сканирането на ириса предлага много по-голяма защита на поверителна информация. По-рано възприето главно на летищата за целите на проверката за сигурност, сканирането на ириса става все по-широко разпространено с множество програми, инсталирани на банкомати във финансовия сектор. Примери за банки, внедрили сканирането на ириса като биометричен идентификатор са Bank of America и National Bank of Qatar (Appinventiv, 2023). Такава банка е и Cairo Amman Bank, която през октомври 2010 г. внедрява технологията за ирисова идентификация на своите банкомати. Разпознаването на ириса е услуга достъпна във всички клонове на Cairo Amman Bank, а в 47 от клоновете на банката, работят банкомати предоставящи на клиентите ирисово разпознаване. Следвайки примера за използване на авангардни технологии през 2011 г. Jordan Commercial Bank също заменя нуждата за лични идентификационни карти при банкови операции с интегриране на системата за разпознаване на ириса (RetailBankerInternational, 2011).

Поведенческата биометрия е иновативен подход за удостоверяване на потребителя, базиран на създаването на уникален профил за всеки клиент. В контекста на онлайн и мобилното банкиране решенията за поведенческа биометрия дават възможност на човек да бъде надеждно идентифициран според неговите навици и средата, в която обикновено извършва транзакции (Security, 2022). Технологията за поведенческа биометрия използва еволюцията на изкуствен интелект (AI) и машинно обучение (ML), за да разпознава и запомня уникални модели на човешко поведение. Физическата биометрия като пръстови отпечатъци, лицево и гласово разпознаване, както и ирисовото сканиране разчита на неизменни биологични характеристики. Поведенческата биометрия изучава динамични, индивидуални действия - като начина, по който човек пише, скоростта, с която плъзга по сензорния екран или движенията на мишката (Banga, 2021). Тези на пръв поглед обикновени дейности съдържат огромни масиви от уникални данни, които могат да разграничат легитимния потребител от такъв с измамни намерения и то с впечатляваща точност. Поведенческите биометрични данни, когато са правилно анализирани и приложени, могат да послужат като безценна помощ в борбата срещу финансови престъпления

Заключение

Нововъзникващите предимства за банките, предизвикани от технологичния напредък, излагат кредитните институции и потребителите на техните услуги на рискове от финансови престъпления. Осъзнавайки реалните и потенциални опасности в пробиви на сигурността банковите институции насочват усилията си към внедряване на иновативни подходи и техники за защити от кибератаки и неправомерни посегателства над наличната им чувствителна информация. Инициативите и насочените ресурси на трезорите за по-ефективна защита, обаче, не са гарант за абсолютна протекция и отпор на злонамерени деяния. Клиентите, като преки участници в банковите операции, също трябва да съблюдават за максималната безопасност на извършваните от тях процеси и да имат гъвкавостта и адаптивността да приемат иновативните техники за сигурност предоставяни им от обслужващите им банки.

References

1. Acharya, S., Polawar, A. and Pawar, P.Y. (2013) Two factor authentication using smartphone generated one time password. *IOSR Journal of Computer Engineering* (IOSR-JCE), 11(2), 85-90. [Online]. Available from: https://www.iosrjournals.org/iosr-jce/papers/Vol11-issue2/L01128590.pdf. [Accessed 07/09/2023].
2. Adlumin (2023) *What is a Spoofing Attack? How Financial Institutions are Being Targeted Security* [Online]. Available from: https://adlumin.com/post/what-is-a-spoofing-attack-how-financial-institutions-are-being-targeted/. [Accessed 17/09/2023].
3. Airehrour, D., Vasudevan N. N., Madanian, S. (2018) *Social Engineering Attacks and Countermeasures in the New Zealand Banking System: Advancing a User-Reflective Mitigation Model* [Online]. Available from: https://www.researchgate.net/publication/324948500_Social_Engineering_Attacks_and_Countermeasures_in_the_New_Zealand_Banking_System_Advancing_a_User-Reflective_Mitigation_Model. [Accessed 02/08/2023].
4. Appinventiv (2023) *Unlocking the Potential of Biometrics Technology in Digital Banking* [Online]. Available from: https://appinventiv.com/blog/biometrics-technology-in-digital-banking/. [Accessed 07/10/2023].
5. Banga, L., Samaya Pillai, C. (2021) Impact of Behavioural Biometrics on Mobile Banking System. *Journal of Physics: Conference* Volume 1964, Advances in Computational Electronics and Communication Engineering, pp. 7-8 [Online]. Available from: https://iopscience.iop.org/article/10.1088/1742-6596/1964/6/062109/pdf. [Accessed 07/09/2023].
6. Boston Consulting Group (2019) *Global Wealth 2019: Reigniting Radical Growth* [Online]. Available from: https://web-assets.bcg.com/img-src/BCG-Reigniting-Radical-Growth-June-2019_tcm9-222638.pdf. [Accessed 05/10/2023].
7. CSI (2022) *2022 BANKING PRIORITIES Executive* Report, pp. 20 https://go.csiweb.com/rs/996-ERF-896/images/WP_CSI_BankingPriorities2022.pdf
8. Das, A., Bonneau, J., Caesar, M., Borisov, N. and Wang, X. F. (2014) *The tangled web of password reuse, in Network and Distributed System Security Symposium* (NDSS), pp. 23–26. [Online]. Available from: https://www.researchgate.net/publication/269197028_The_Tangled_Web_of_Password_Reus. [Accessed 07/10/2023].
9. Deloitte (2016) *Ransomware Holding Your Data Hostage* [Online]. Available from: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-ransomware.pdf. [Accessed 12/10/2023].
10. DevX (2023) *IP Spoofing* [Online]. Available from: https://www.devx.com/terms/ip-spoofing/
11. Digital Guardian (2018) *What is Social Engineering? Defining and Avoiding Common Social Engineering Threats* [Online]. Available from: https://www.digitalguardian.com/blog/what-social-engineering-defining-and-avoiding-common-social-engineering-threats?_gl=1*9in287*_ga*OTQ1NDM4MTU2LjE3MDA5OTcxODE.*_ga_NHMHGJWX49*MTcwMDk5NzE4MC4xLjEuMTcwMDk5ODIyNC42MC4wLjA.*_ga_Q142HN6432*MTcwMDk5NzI3MC4xLjEuMTcwMDk5ODIyNC42MC4wLjA. [Accessed 07/10/2023].
12. Digital Guardian (2023) *What are Social Engineering Attacks? (Types and Definition)* [Online]. Available from: https://www.digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent attack?_gl=1*osjws6*_ga*OTQ1NDM4MTU2LjE3MDA5OTcxODE.*_ga_NHMHGJWX49*MTcwMDk5NzE4MC4xLjAuMTcwMDk5NzE4MC42MC4wLjA. [Accessed 15/09/2023].
13. Eurofins (2021) *Eurofins Cyber Security* https://www.eurofins-cybersecurity.com/news/security-threats-bankingfinance/. [Accessed 07/10/2023].

14. Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T. & Koucheryavy, Y. (2018). *Multi-factor authentication: A survey. Cryptography, 2*(1), pp.1-2.
15. Petrescu, Relly Victoria, (2019) Face Recognition as a Biometric Application *Journal of Mechatronics and Robotics 2019*, Volume 3: 237.257, [Online]. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3417325. [Accessed 07/10/2023].
16. Phonexia (2021). *Voice Biometrics in the Banking Industry* [Online]. Available from: https://www.phonexia.com/blog/voice-biometrics-in-the-banking-industry. [Accessed 27/10/2023].
17. Rafailov, D., Vachkov. S., Georgiev, L., Kirov, S., Valkanov, N., Naydenova, K., Dzhaparov, P. (2020). *Finansovata infrastruktura - sustoyanie, problemi, inovativen potencia*. Varna: Nauka i ikonomika.
18. Retail Banker International (2011). *Jordan CommercialBank applies Iris recognition system for banking [*Online]. Available from: https://www.retailbankerinternational.com/news/jordan-commercial-bank-applies-iris-recognition-system-for-banking/?cf-view. [Accessed 18/09/2023].
19. Security (2022) *Banking & behavioral biometrics: Understanding privacy & security regulations* [Online]. Available from: https://www.securitymagazine.com/articles/98506-banking-and-behavioral-biometrics-understanding-privacy-and-security-regulations. [Accessed 07/10/2023].
20. Sekhar, S. C, Kumar M. (2023). *An Overview of Cyber Security in Digital Banking Sector*, vol. 2, no. 1, pp. 44 [Online]. Available from: https://journal.formosapublisher.org/index.php/eajmr/article/view/1671/2115. [Accessed 14/10/2023].
21. Sophos (2023). *The State of Ransomware in Financial Services 2023* [Online]. Available from: https://assets.sophos.com/X24WTUEQ/at/skqcw8qv736cwr5hmtkxfwg/sophos-state-of-ransomware-financial-services-2023-wp.pdf. [Accessed 07/10/2023].
22. The Guartian (2014). *Forget fingerprints – banks are starting to use vein patterns for ATMs* [Online]. Available from: https://www.theguardian.com/money/2014/may/14/fingerprints-vein-pattern-scan-atm. [Accessed 07/10/2023].
23. TrendMicro (2021). *Attacks from All Angles: 2021 Midyear Security Roundup* [Online]. Available from: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat reports/roundup/attacks-from-all-angles-2021-midyear-security-roundup
24. Venkatraman S., Delpachitr, I. (2008). *Biometrics in banking security: A case study*, Information Management & Computer Security, vol. 16, no. 4, pp. 415-430 Online]. Available from: https://www.academia.edu/62078148/Biometrics_in_banking_security_a_case_study. [Accessed 07/10/2023].