ЗАЩИТА СРЕЩУ ИЗМАМИТЕ ПРИ ЕЛЕКТРОННИТЕ РАЗПЛАЩАНИЯ В ТЪРГОВИЯТА

Доц. д-р Михал СТОЯНОВ
Икономически университет, Варна
E-mail: michal.stojanov@ue-varna.bg

Резюме: *Последните десетилетия са белязани от непрекъснатото развитие на информационните и телекомуникационните технологии, които имат сериозно влияние върху местното, националното и глобалното стопанство. Тяхното приложение създава и трансферира стопански и социални ефекти за икономическите агенти, но се съпътства и със сериозните изпитания на сигурността на използването на дигиталните технологии. Едно от усложняващите се проблемни измерения са нарушенията при осъществяване на платежни операции при търговски сделки. В настоящата работа е направен преглед на същността на престъпленията при разплащания в реална и цифрова търговска среда, особеностите на различните технологични средства за защита при осъществяване на електронни разплащания и някои възможности за подобряване на персоналната безопасност при плащания в търговията и работа в Интернет.*

Ключови думи: *електронни разплащания, токън устройства, електронен подпис, биометрични данни, HTTPS.*

JEL: *D18, L81, E42, K14.*

Въведение

Протичащата дигитална трансформация постепенно превръща рутинни ежедневни операции в напълно автоматизирани процеси с висока бързина, комплексност на обслужването и редукция на човешките грешки. Едно от предизвикателствата в този процес е опазването на сигурността на дигиталната информация. Особено важен и чувствителен е този момент при осъществяването на електронни разплащания. При тях равнището на сигурност изисква, управлението на разплащането да бъде оторизирано посредством адекватно удостоверяване на самолич-

ността на платеца и получателя на паричните средства. Това следва да бъде реализирано без особени усилия от участниците и при минимум изразходване на ресурси и основно на фактора време. Усъвършенстването на този процес предполага използване на защити от по-високо ниво, като например динамично електронно удостоверяване, електронен подпис, биометричните данни на платеца и интернет протоколи за криптиран информационен обмен.

Настоящата работа има за своя основна цел да разгледа същността на измамите при разплащания и особеностите на различните технологични средства за защита при осъществяване на електронни разплащания в реална и цифрова търговска среда. Постигането на тази цел предполага решаването на следните по-важни задачи:

1. Обобщаване и анализиране на теоретичните аспекти на престъпленията и защитата при електронните разплащания.

2. Систематизиране на придобилите най-широка популярност инструменти за защита при електронни платежни операции в цифрова среда.

3. Анализ на националната и глобалната картина на финансовите престъпления и прилагането на официална политика за информационна сигурност на българските предприятия и извеждане на възможности за защита срещу измами при електронни разплащания в търговията.

Съвременното общество и неговите икономически субекти използват множество платежни средства и системи, така постепенната доминация на разплащанията в брой бива изместена от електронни разплащания. Въпреки това всяка една от тези конвенционални или цифрови алтернативи реализира динамични стратегии, обвързани със защита до определено, приемливо за всички участници равнище. Нещо повече, сериозната популярност на електронната и напоследък мобилната търговия предполага усъвършенстване на технологични средства за защита на плащанията и свързаната с тях персонална информация на потребителите.

1. Теоретични аспекти на защитата и престъпленията при електронните разплащания

При създаването на едно платежно средство отговорността за неговата защита най-често се гарантира от този, който го издава, но постепенно и най-вече в наши дни ангажираността за поддържането на сигурността става споделена и включва цялата съвкупност от участници в платежния процес. Така освен от оператора на разплащателната система всички обвързани нейни потребители могат да се присъединят в механизма на противодействието срещу опитите за зловредни действия и подобра индивидуална защита. По този начин освен чрез физическа охрана, криптиране и защита сигурността на съвременните разплащания може да

бъде гарантирана и посредством разпределение на чувствителната информация. Това означава, че участниците в разплащанията: платец, получател и посредници могат ефективно да контролират автентичността и валидността на уязвимите данни. Всъщност посредством добавянето на непредвидим или уникален компонент кой да е от членовете може да създаде допълнителна сигурност и да осъществи самоконтрол по отношение на останалите и цялата трансакция. Подобна относителна децентрализация съществено редуцира опитите за еднопосочна атака, тъй като тя би била неефективна по отношение на широкия кръг от участници. Разбира се, в официалните системи за разплащания отговорността на операторите и регулаторните органи на тяхното функциониране е ключова по отношение на ефективната защита на потребителите. Това е заложено и в Директива (ЕС) 2015/2366, която предполага широко въвеждане на персонализирани средства за сигурност, включително и посредством „установяване на идентичността чрез използването на два или повече елемента, категоризирани като знания (нещо, което само ползвателят знае), притежание (нещо, което само ползвателят притежава) и характерна особеност (нещо, което характеризира ползвателя), които са независими, така че нарушаването на един елемент не влияе на надеждността на останалите, а процедурата е разработена по начин, който защитава поверителността на данните за установяване на идентичност“ (Директива (ЕС) 2015/2366 на Европейския парламент и на Съвета на Европейския съюз, 2015). Едновременното или последователното прилагане на отделните защитни елементи повишава сигурността на цялата трансакция и гарантира нейната устойчивост срещу неправомерни въздействия и външни атаки. В подобна ситуация потребителите могат да се почувстват по-сигурни в платежния процес и това да повлияе на общата удовлетвореност от търговското посещение и склонността за покупки. Така например желанието „потребителите да купуват по интернет ще е само, ако се чувстват комфортно и сигурно в средата и възприемат електронната търговия като съгласувана със своите ценности и начин на живот“ (Matsuo & Colomo-Palacios, 2013, p. 118). Еднозначно, ако потребителят задоволи своята потребност от сигурност, той редуцира комплекса от фактори, които задържат собствената му склонност да участва в търговския обмен и да развива собственото си потребление. Така например, при електронната търговия, отсъствието на рискове, свързани с плащането, може да стимулира потребителя да отдели повече време и внимание върху останалите елементи на търговското посещение.

Кражбата по действащия в България Наказателен кодекс (Наказателен кодекс, 2017), се определя като „отнемане на чужда движима вещ от владението на другиго без негово съгласие с намерение противозаконно да я присвои“ (Раздел I от НК), докато измамата е причиняване на имотна вреда, като се използва заблуждение, неопитността или неосведомеността на някого (Раздел IV от НК). Тези две престъпления против собствеността свързваме с целенасочените действия за злоупотреба с

чужда собственост и нейното незаконосъобразно придобиване от нарушителя. Кражбата е причиняване на имуществена вреда без знанието на собственика, докато при измамата той е въведен целенасочено в ситуация, при която възникването на неблагоприятните ефекти се причинява от собствените му действия, продукт на заблуждението, в което е бил поставен. Примерни ситуации за реализацията на тези закононарушения при търговски обмен са, когато клиентът стане жертва на кражбата на данни за използвани от него безналични платежни инструменти или споделянето на информация за тях при пазаруване във фалшиви интернет-страници, имитиращи компании, с утвърден пазарен имидж и репутация.

Като самостоятелна група и по-широко се определят престъпленията към паричната и кредитната система, квалифицирани като препravяне на парични знаци и платежни инструменти (чл. 243 от НК). Директният израз на този престъпен състав е умишленото компрометиране на защитните елементи, които предпазват интегритета на платежните средства. Допълнително той се конкретизира в „използването на платежния инструмент и информацията, свързана с него, без съгласието на титуляря“ (чл. 249 от НК). Едновременно тук се преследват и „изготвянето, монтирането и използването на технически средства за придобиване на информация за съдържанието на платежния инструмент“ (чл. 249 от НК). Това означава, че обхватът на престъпното посегателство е по отношение на всеки противоправен и умишлен опит за достъп до чувствителна информация, който води до зловредни икономически ефекти и затова се посочват като престъпления против стопанството. Те имат директно отношение към съвременните безналични способи за разплащания, които постепенно изместват традиционните платежни средства в търговския обмен. По тази причина се разширява и обхватът на наказателното преследване, за да отговори адекватно на цифровата трансформация в стопанските процеси.

По отношение на използването на компютърни и информационни системи нарушенията са свързани основно с незаконния достъп и използване на компютърни данни в една или повече информационни системи (Глава девета „а“ от НК). Сериозността на престъплението се определя и от степента на вредните последствия и настъпилите други тежки щети от вмешателството без разрешение във функционирането на компютърни системи и мрежи. Нормалното функциониране на отдалечените компютърни системи и мрежи предполага използване на далекосъобщителни мрежи, затова в състава на чл. 348а от НК се определя измамата и другите незаконни начини за използване на тези мрежи, техните съоръжения или услуги, при което имаме несъобразено със закона използване на съобщенията в преносната среда. Това предполага преследване на всяко неправомерно вмешателство в средата за пренос на електронна информация, включително и по отношение на електронните разплащания.

Освен в Наказателния кодекс текстове срещу престъпленията при разплащанията и използването на платежни средства и системи се съдър-

жат в административнонаказателни разпоредби на други специализирани нормативни актове като например, Закон за платежните услуги и платежните системи, Закон за електронните съобщения, Закон за защита на потребителите (ЗЗП), Закон за кредитните институции, Закон за защита на личните данни и др. Следователно законодателят е предвидил множество хипотези, свързани с умишлените измами при реализацията на електронни разплащания в търговията. При това положение, освен посредством преследване и санкциониране на недобросъвестното поведение, участниците в платежния процес разполагат и с други превантивни инструменти за относително ефективна защита. Пример за това е правото на потребителя в „14-дневен срок да се откаже от договора от разстояние или от договора извън търговския обект, без да посочва причина, без да дължи обезщетение или неустойка и без да заплаща каквито и да е разходи, с изключение на разходите за връщането на стоките“ (чл. 50 от ЗЗП (Закон за защита на потребителите, 2018)). Друг пример е Общият регламент за защита на данните на ЕС (GDPR или Регламент (ЕС) 2016/679), който въвежда нови по-високи изисквания към регулирането на неприкосновеността на личните данни. Според регламента, „ефективната защита на личните данни изисква укрепване и подробно описание на правата на субектите на данните и задълженията на онези, които обработват и определят обработването на личните данни, както и еквивалентни правомощия за наблюдение и гарантиране на спазването на правилата за защита на личните данни и еквивалентни санкции за нарушенията“ (Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета на Европа, 2016). Това предпоставя, всяко обработване на лични данни да бъде съобразено с действащото законодателство, прилагано за точно определени и известни на страните цели, съгласувано със субекта на данните или произтичащо от нормативна регулация, при гарантирана прозрачност и възможност, субектът на данните да упражнява своите обезпечени от закона права и пр. Задължителността на Общия регламент за защита на данните на ЕС (GDPR) в рамките на ЕС ще предизвика сериозни промени във всяка една бизнес сфера, включително и в начина, по който търговските организации събират и обработват информация за своите клиенти и в най-висока степен нейната защита. На равнище стопански единици също е предвидена забрана за злоупотреба с „производствени или търговски тайни, които се определят като факти, информация, решения и данни, свързани със стопанска дейност, чието запазване в тайна е в интерес на правоимащите“ (§ 1 т. 9 от Закон за защита на конкуренцията). Подобно положение може да бъде достигнато при действия, противоречащи на добросъвестната търговска практика, които да предизвикат неблагоприятни икономически и други последствия от неправомерно узнаване, използване или разгласяване на защитени от фирмата факти и знания. Тази информация не е задължително да бъде свързана единствено с вътрешнофирмени икономически процеси, но може да бъдат и данни, събрани по отношение на външната микросреда на компанията. Основно това е информация, по

отношение на която стопанският субект встъпва в ролята на администратор на лични данни. Това отново поставя акцент върху важната предпоставка, участниците в икономическия процес, които обменят или имат достъп до подобна информация, да са предвидили и да прилагат мерки за нейната защита. В този контекст установяването на нелоялно поведение между бизнес партньори или конкуренти може да бъде санкционирано от Комисията за защита на конкуренцията след подаване на искане, образуване на производство, проучване и приемане на решение за установено и доказано закононарушение. Посочените примери демонстрират широките възможности за възникване на ситуации, които пряко или косвено могат да увредят интереса на участниците при електронните разплащания в търговията.

В най-общ план съществуват множество обобщаващи критерии, по които може да бъде направено разграничение на видовете измами при електронни разплащания (табл. 1).

Таблица 1
Класификация на видовете измами при електронните разплащания

Класификационен критерий	**Видове измами**
Според степента на разпространеност в електронна среда (Juniper Research, 2016, pp. 13-15)	• Чиста измама (clean fraud); • Похищаване на клиентска сметка (account takeover); • Измама, свързана с рекламация на банковото плащане и връщане на пари след реално получаване на продуктите (friendly fraud); • Похищение на идентичността (identity fraud); • Измами от съдружници (affiliate fraud); • Препращане (re-shipping) е измамна схема за прехвърляне на незаконно придобити активи посредством информиран или невинен посредник, т.нар. „муле“; • Ботнет (botnets) е компютърна мрежа и/или зловреден софтуер, които работят в автономен режим и имат за цел кражба на лични данни; • Фишинг атака (phishing) представлява използването на измамнически уебсайтове или получаването на измамнически електронни съобщения под формата на „предупреждения от банки или други организации, с които потребителят има взаимоотношения“ (Гайдаров, 2018); • Уейлинг (whaling, spear phishing) е таргетиран към определени лица фишинг; • Фарминг (pharming) е пренасочването на трафика на официален уебсайт и/или незаконен сайт, където клиентите несъзнателно въвеждат своите лични данни; • Триангулация (triangulation) е кражбата на информация за дебитни и кредитни карти посредством технологията на онлайн търгове, сайтове за продажба на билети или онлайн обяви.

Според вида на заплахите/атаките, засягащи областта на плащанията (European Payments Council, 2018)	• За отказ на услуга (Distributed Denial of Service - (D)DoS); • Социално инженерство (social engineering); • Опитите за фишинг (phishing); • Зловреден софтуер (malware); • Прогресивни целенасочени атаки (Advanced Persistent Threats – APTs); • Атаки, свързани с мобилни устройства (mobile device related attacks); • Ботнети (botnets); • Заплахи, свързани с облачни услуги и големи данни (threats related to cloud services, big data); • Заплахи, свързани с Интернет на нещата (Internet of Things – IoT); • Заплахи, свързани с виртуални валути (virtual currencies); • Измами, свързани с платежните карти; • Измами, свързани с терминалните АТМ устройства (банкомати).
В зависимост от фазата на търговската сделка, която се засяга от измамата	• Преди продажбата: фалшиви търговци, представяне на нереални условия на търговския обмен, въвеждане в заблуждение и др.; • По време на продажбата: измами с кредитни карти и платежни средства при закупуването на продукта, промяна на условия на сделката и др.; • След продажбата: измами, свързани с доставката, измами, свързани с връщането на продукта и др.
Според териториалния обхват и субекта на измамата (Kratcoski, Dobovsek, & Edelbacher, 2015, p. 30)	• Вътрешна (национална) • Международна
Според насочеността на измамата (Dalla & Geeta, 2013)	• Срещу личността • Срещу собствеността • Срещу държавата • Срещу обществото
Според субекта на измамата (Bernard, et al., 2017, p. 14)	• Срещу физическите лица / гражданите • Срещу юридическите лица / бизнеса и организациите
Според тежестта на престъплението чл. 49, т. 7, 8 и 9 от НК (Наказателен кодекс, 2017)	• „Маловажен случай“ е този, при който извършеното престъпление с оглед на липсата или незначителността на вредните последици или с оглед на други смекчаващи обстоятелства представлява по-ниска степен на обществена опасност в сравнение с обикновените случаи на престъпление от съответния вид. • „Тежко престъпление“ е това, за което по закона е предвидено наказание лишаване от свобода повече от пет години, доживотен затвор или доживотен затвор без замяна. • „Особено тежък случай“ е този, при който извършеното престъпление с оглед на настъпилите вредни последици и на други отегчаващи обстоятелства разкрива изключително висока степен на обществена опасност на деянието и дееца.

Посочените по-общи и специфични критерии демонстрират изключителната комплексност и непрекъснатата изменчивост на проблема на измамите при електронни разплащания, което налага системно актуализиране на инструментите за противодействие. Това може да бъде постигнато посредством постоянно наблюдение и актуализиране на организационните и технологичните средства и защити за предотвратяване на измамите при електронни разплащания в търговията.

2. Инструменти за защита при платежни операции в цифрова среда

Всяка една платежна операция, определена като „действие, предприето от платеца или от получателя по внасяне, прехвърляне или теглене на средства, независимо от основното правоотношение между платеца и получателя“ (Допълнителни разпоредби на Закона за платежните услуги и платежните системи, 2017), трябва да бъде обезпечена с определено ниво на защита. При платежните операции с налични средства физическата проверка позволява, участниците да осъществяват тотален контрол в мястото на тяхното осъществяване. На практика това се реализира посредством ръчна или автоматизирана проверка на вградените високотехнологични защитни елементи в съвременните платежни средства. Обратно, при електронните платежни операции и основно при тези, осъществявани изцяло в електронна среда, механизмите на защита изискват адекватни дигитални иновации и допълнителни механизми за контрол и сигурност.

Ще разгледаме най-популярните технологични решения за защита при безналични разплащания, използвани в настоящето, както и възможностите за тяхното бъдещо развитие:

• Използване на защитен https мрежов протокол за пренос на данни в интернет среда (HyperText Transfer Protocol Secure). С оглед повишаване на сигурността при работа в Интернет между краен потребител и уебсървъра на търговеца се създава връзка, която позволява криптиран трансфер на информацията в мрежата. Посредством този протокол данните, изпратени в глобалната мрежа, се кодират и само предварително идентифицирани участници в техния обмен имат възможност да ги разчетат. По този начин чувствителната потребителска информация или цялото потребителско поведение в интернет може да бъде защитено от злонамерено и неоторизирано проследяване и манипулиране. Потвърждаването на идентичността на страните се извършва с помощта на SSL (Secure Socket Layer) сертификат, който се добавя към протокола за пренос на информацията и позволява само на крайните участници в електронния информационен обмен да изградят сигурна връзка, защитена срещу неоторизирано прихващане. Това позволява на клиентите на електронната

търговия да изградят цифрово доверие към партниращия агент на обмена, който им осигурява надеждна среда за сигурна размяна на информация. Положителното на този механизъм е, че той протича на заден план в интернет комуникацията и онлайн потребителят не е обвързан с неговото автоматично функциониране. Това позволява, той да насочи своето внимание към преживяването, свързано с електронното пазаруване, но ако пожелае, може да проконтролира сигурността на връзката, самоличността на използвания сертификат и надеждността на организацията, която удостоверява идентичността на търговеца посредством неговия домейн или уебсайт. В глобалната мрежа най-популярните сертифициращи органи в края на 2017 г. според W3Techs (Gelbmann, 2018) са Comodo, IdenTrust и DigiCert Group. Така, независимо от операционната система и характеристиките на използвания хардуер, съвременните приложни програми за преглед на информационно съдържание в интернет създават относително безопасна среда за онлайн търговско преживяване. Последното дава възможност, вниманието на клиента да бъде върху предлаганите от търговеца продукти, техните характеристики и условия на размяната, а не разсейвано от несигурността на разплащането и рисковете за използването на личните данни. Допълнителна възможност е използването на SET (Secure Electronic Transactions) протокол, при който чувствителната информация за използваните виртуални платежни средства, която се разменя между участниците клиент, търговец и платежни институции във виртуалния търговски обмен, е с ограничен до необходимото достъп за всеки един от тях. Ключовият компонент на механизма на неговото функциониране свързваме с определящата роля и ангажираност на операторите на платежни системи, което едновременно усложнява и ограничава неговото приложение и популярност в реалната търговска практика в сравнение с условно по-достъпния SSL протокол.

• Токън устройства. Това са специални миниатюрни устройства, които могат да получават, съхраняват и изпращат цифрови ключове за оторизиране на определени операции. Като самостоятелни цифрови апарати те могат да бъдат окомплектовани с различни компоненти, които да им позволят да комуникират с други устройства и системи или да визуализират оторизиращи ключове. Те се предоставят от обслужващия платеца доставчик на платежни услуги за целите на дистанционното разрешаване на операции за електронно заплащане на закупени продукти в цифрова среда. Устройствата могат да генерират уникални идентификатори, които да бъдат използвани еднократно или за лимитирани интервали от време, при което ограниченият им живот е допълнителна предпоставка за повишаване на сигурността. Тяхното приложение е надграждаща стъпка по отношение на традиционните методи за защита, които включват персоналните данни на платеца. Така, освен чрез зададена от потребителя статична комбинация от букви, цифри или символи за удостоверяване на плащането, ще се приложи и допълнителен статичен или динамичен ключ, зададен или трансфериран от оператора на платежната

система или обслужващата платеца институция. Разбира се, вместо използване на специално токън устройство, този ключ може да бъде получен от потребителя и чрез предпочитан от него алтернативен комуникационен канал – електронна поща, SMS услуга на мобилните оператори и др. Това позволява в съвременните умни телекомуникационни устройства да се емулира както класическата банкова карта, така и токън устройството и те да се превърнат в основен компонент на защитените разплащания в реалната и виртуалната търговия. Освен това тяхното приложение може да бъде и напълно неангажиращо времето и вниманието на потребителя, като е достатъчно да ги прикачи към потребителския интерфейс на използвания за извършване на разплащането хардуер. Дори при използване на комуникация от близък (непосредствен) контакт NFC (Near Field Communication) между устройствата физическото им свързване не е необходимо.

• Електронен подпис. По своята същност това са „данни в електронна форма, които се добавят към или са логически свързани с други електронни данни, и които се използват като метод за удостоверяване“ (Директива 1999/93/ЕО на Европейския парламент и на Съвета на Европа, 2000) и могат да се прилагат от титуляря на електронния подпис, за да се подписва (Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета на Европа, 2014). Това определя електронния подпис като инструмент за защитен обмен на информация, който гарантира автентичност, цялостност, конфиденциалност и неотменяемост на волеизявленията на притежателя на електронния подпис в цифрова среда при осъществяването на специфични видове електронни операции и дейности. Посредством неговото прилагане всяко електронно изявление, към което се добавя електронен подпис, се възприема и има значението на саморъчен подпис с равна правна сила, когато това е уговорено между страните чл. 13 от Закон за електронния документ и електронните удостоверителни услуги (Закон за електронния документ и електронните удостоверителни услуги (загл. изм. - дв, бр. 85 от 2017 г.), 2017). Използването на електронен подпис позволява да се разшири кръга на търговските сделки, които могат да се осъществят с отдалечен достъп и от разстояние, независимо от изискването за задължително формализиране на акта на покупко-продажбата. Така силата и последствията от използването на електронен подпис са равнозначни с това на персоналното волеизявление в акта на действителното подписване. Наред с това позитивите от приложението на електронния подпис са свързани с неговата публична част, която може да бъде проверена от получателя на документа.

• Биометрични данни. Съвременните умни устройства (компютри, телекомуникационни апарати и др.) все по-масово се конфигурират с компоненти, позволяващи, потребителите да се идентифицират посредством използване на биометрични данни. Съгласно Закона за българските лични документи, биометричните данни се определят като „изображението на лицето на гражданина и пръстовите му отпечатъци, които се използват за

разпознаване и проверка на заявена самоличност“ (Закон за българските лични документи (загл. изм. - ДВ, бр. 82 от 2009 г.), 2017). По този начин потребителите могат да се идентифицират, като използват уникалните и неповторими характеристики на своята физиологическа индивидуалност. Това дава възможност, чрез пръстови отпечатъци (дактилоскопия) и/или лицево, гласово и друго биометрично разпознаване на потребителя да се установи самоличността еднозначно при пазаруване и разплащане. Валидирането посредством биометрични данни дава възможност да се достигне най-високо ниво на защита на собствените ресурси в мястото на продажбата и при плащане. Технологията на тяхното използване предполага много по-големи нива на защита както по отношение на прилаганите алгоритми и устройства, така и в сравнение с другите алтернативи за защита на плащанията. Нещо повече, биометричната технология се свързва с предимства за всички участници в разплащанията, като „подобрява преживяването и гарантира сигурността на трансакцията при пазаруване“ (Perez, 2018), независимо от мястото на продажбата. Последното е израз на възможността, процесът на разплащане да бъде оптимизиран в няколко аспекта, но основно по отношение на сигурността и необходимото време за осъществяване. Приложението на биометрията има изключително сериозен потенциал при електронните и мобилните форми на търговия. Това състояние се предопределя благодарение на вградените технологии в съвременните преносими компютри, таблети, смарт телефони и други, които разполагат като минимум с камера, вградени микрофони, а по-новите и с четци за пръстови отпечатъци. Така биометричната идентификация по време на електронната или мобилната продажба оптимизира крайния процес на обмена, свързан с цифровата трансакция. В тази фаза изключително значими остават моментите за премахване на несигурността, потенциалните заплахи за безопасността по веригата на плащането и гарантирането на всеобхватната защита на участниците в платежния процес. Така чрез биометричната оторизация и валидизация се установява идентичността на клиента за операцията на плащането при електронната и мобилната търговия, където се създава защитен виртуален мост между интернет страницата на търговеца или доставчика на платежни услуги и платеца, така както се изисква в Директива (ЕС) 2015/2366. Биометричното удостоверяване безпроблемно може да се прилага при всяка форма на магазинна търговия с подходящото оборудване в точката на продажба, обезпечено с умения и компетенции от страна на обслужващия търговски персонал и познание на клиента за използването на технологията.

Представените решения са част от механизмите, чрез които може да се гарантира установяването на идентичността на клиента и осъществяваните от него операции при електронни разплащания в реална или виртуална среда, където съществуват рискове от възникване на кражби, измами и злонамерени действия на трети страни. Те поставят акцент върху сигурността на платежните услуги посредством идентичността на

участниците. Механизмите на функциониране гарантират, че преди, по време и след осъществяване на платежната операция, независимо от мястото и времето на нейното реализиране, остават записи, които позволяват установяване на заангажираните лица и проследимост на информационните и паричните потоци. Нещо повече, идентификацията и автентификацията е актуалният подход за борба срещу измамите при плащания в търговията. Всъщност, колкото повече са нивата на защита и колкото побързо протичат удостоверителните процеси, по-комплексна е удовлетвореността на участниците в търговския обмен и сигурността за техните платежни сметки.

Прилагането на инструменти за защита при платежни операции в електронна среда изисква, участващите страни, като получатели на чувствителна информация, и лицата, които имат контакт и възможност за преглед на подобни данни, да имат съответните права на достъп, разрешено равнище на обработка и защита на извършваните от тях дейности. Това определя ролята им на администратори на данни, както и правата и задълженията при операциите, свързани с електронни разплащания. В тази връзка на допълнителна защита подлежи както инфраструктурата, обезпечаваща преноса на информацията за платежни операции, така и крайните устройства за достъп и работата със системите за платежни операции. От една страна, за защита тук се прилагат съвременни технологични решения, а от друга, установената организация на електронните платежни операции. Най-популярното технологично решение са защитните стени (firewall), които в зависимост от своята комплексност могат да бъдат реализирани като хардуерни, софтуерни или техни комбинирани решения за непрекъсната автоматизирана проверка на входящия и изходящия поток от данни към и от електронната платежна система. Основната цел на всяка една защитна стена е да осъществява неизменна по определени правила проверка и да позволява или ограничава входящия и изходящия информационен обмен, който се или не се подчинява на установените норми. За физическите лица с достъп до крайни устройства, които са елемент на електронните платежни системи, може да бъде използван формалният режим на издаваните свидетелства за съдимост при постъпване на работа съгласно чл. 1 (1) т. 5, Наредба № 4 за документите, които са необходими за сключване на трудов договор (Министерство на труда и социалната политика, 2017). Това обезпечава организациите, търсещи служители, както и в предвидените от законодателството случаи с превантивен инструмент, обвързан с прилагане на изискването за свидетелство за съдимост по отношение на определен кръг лица с достъп и работещи със системи за електронни разплащания. Допълнително при извършването на операции с крайни устройства на електронни платежни системи е целесъобразно да се прилага политика за двуфакторна или по-висока автентикация. Това може да се осъществи с помощта на U2F (Universal 2nd Factor) устройства, които са индивидуални за всички потребители с права на достъп. Допълнително, като стандарт, се въвежда ограничение

на достъпа до определени части на системата извън рамките на определени физически места и по определени правила, като отдалеченият достъп може да бъде осъществен посредством използване на подходящия тунелиращ протокол за работа във виртуална частна мрежа, като например PPTP, L2TP, OpenVPN, SSTP, IKEv2 (Фоукс, 2016). Всичко това позволява да се постигне по-висока степен на защита и контрол на достъпа до системата за електронни разплащания и при работа с личните данни на физическите лица, които са участници в електронния търговски обмен.

3. Проблеми на защитата срещу измами при електронните разплащания в търговията

Еволюцията на платежните системи и технологичните иновации, които ги съпътстват, са в основата на подобрените условия за търговски обмен и неговата миграция в цифрова среда. В настоящето реалността от приложението на изкуствен интелект позволява да се извлекат позитиви и по отношение на защитата срещу измами при продажбите. Това означава, че интелигентните и автоматизирани аналитични системи наблюдават непрекъснато потребителската активност и могат да реализират коригиращи действия в реално време, да откриват нови и неизвестни схеми на злоупотреби в търговията и разплащанията. Машинното обучение, в комбинация с изкуствения интелект, може да предложи решения, посредством които търговският цикъл да бъде икономически и социално по-ефективен. Направленията на приложение на машинното обучение се разгръщат в областта на усъвършенстването на веригата на доставки, изучаването на потребителското поведение и борбата с измамите при платежни операции в търговията. Последните най-често са свързвани с финансовите измами, които като глобална пандемия засягат все повече лица. Така например през 2016 г. жертви на подобен род престъпления само в САЩ са били 15,4 млн. граждани, нарастването на годишна база е с 16% и се измерва с кражбата на 16 млрд. щ.д., което е увеличение от почти 1 млрд щ.д. на годишна база (Miller, Marchini, & Pascual, 2017). Загубите от измами с карти в Европа през 2016 г. достигат обем от 1,8 млрд. евро, като най-засегнатите държави са Обединеното кралство и Франция, които заедно формират дял от почти три четвърти от този род престъпления в Европа (Ecommerce news, 2017). Това автоматично определя защо за половината европейски онлайн купувачи безпокойството за измамите е основната пречка пред онлайн плащанията (Masterindex 2017, 2017, p. 7). В Република България през 2017 г. общият брой на престъпленията против собствеността е 5 882 бр., като 65,1% от тях или 3 827 бр. са определени като кражби, 10,6% или 623 бр. са класифицирани като грабеж, допълнително за същия отчетен период 377 бр. са престъпленията против паричната и кредитната система (Национален статистически институт, 2018). За сравнение преди 7

години или през 2010 г. са отчетени 8 973 бр. кражби и 1 114 бр. грабежи при общо 12 538 бр. престъпления против собствеността и 257 бр. престъпления против паричната и кредитната система. Редукцията в броя на престъпленията против собствеността с 6 656 бр. или понижение с 53% се съпровожда с ръст от 146,7% при престъпленията против паричната и кредитната система. Положителна е и промяната при проблемите, които българските граждани срещат при осъществяване на търговски обмен по интернет, където относителният дял на лицата, засегнати от измама през 2017 г. е 0,3% от гражданите, докато през 2004 г. делът е бил 2,9% (Национален статистически институт, 2017). Най-много са били ощетените от измами при поръчки или покупки на стоки и услуги в глобалната мрежа през 2006 г., когато 3,7% от участвалите в онлайн обмен български лица са декларирали, че са били неблагоприятно засегнати от измамите в електронна среда. В глобален мащаб стойностното измерение на щетите, причинени от докладвани киберпрестъпления към Центъра за подаване на жалби за престъпления в интернет на Федералното бюро за разследване на САЩ са с най-високо значение от 1 450,7 млн. щ. д. през 2016 г., при последна оповестена стойност от 2017 г. в размер на 1 418,7 млн. щ. д. (Federal Bureau of Investigation, 2018, p. 4), което съотнесено към 2001 г., когато причинените щети от престъпления в цифрова среда са били със стойност от само 17,8 млн. щ. д. посочва нарастване от над 79 пъти (The National White Collar Crime Center, Bureau of Justice Assistance, Federal Bureau of Investigation, 2008, p. 3). Това определя киберпрестъпността като проблем с разрастващо се глобално значение. На този фон е логична констатацията, че „в рамките на ЕС повече от една десета от потребителите на интернет вече са ставали жертва на онлайн измами“ (Европейска Комисия, 2013, стр. 3). Едновременно с това следва да се отбележат три важни проблема на публичната информация за реалните измерения на престъпността при електронните разплащания в търговията. Първият е свързан с това, че съществена част от извършените измами при цифрови разплащания остават необявени или нерегистрирани от жертвите. Вторият е, че делът на измамите, които остават извън официалната отчетност, поради условно несъществената материална вреда, е значителен. Третият проблем е, че еволюцията на организираната престъпност изпреварва усъвършенстването на защитните системи. Това се дължи основно на ограничената ресурсна обезпеченост за осъществяване на системни хардуерни и софтуерни подобрения. Тази нова реалност изисква алтернативни методи за противодействие и сигурност, което води до появата на нов клас електронни услуги, свързани със защитата на информацията при дигитални разплащания в търговията. Въпреки това, всеки потребител има възможност да подобри собствената си безопасност при е-плащания в търговията, като най-разпространените препоръки за борба с тези форми на организирана престъпност са (ГДБОП-МВР, 2018):

• Информиране на платежната институция, която обслужва компрометираните платежни сметки на потребителя. Бързината на контакта и

пълнотата на информацията за регистрираното необичайно събитие стартира стандартни протоколи за защита на интересите на потребителя и платежната институция.

• При установяване на кражба на лични данни и документи, пряко или косвено свързани с платежни инструменти, потребителят следва да информира обслужващата платежна институция и контролните органи за защита на личните данни и борба с престъпността.

• Системно следене на движенията по платежни сметки, активиране на електронно известяване чрез електронна поща или SMS услуга на мобилните оператори за заявени и/или осъществени активни операции със собствени платежни средства. При регистрирани незаявени плащания или необичайни трансакции потребителят следва да изиска подробна информация от обслужващата платежна институция и да предяви коригиращи действия и рекламация.

• При установяване на злоупотреби или необичайна активност от потребителски акаунт, създаден към търговец, е желателно да се подаде сигнал за компрометирането на клиентската сметка или профил. При по-усъвършенстваните платформи за електронна търговия е създадена възможност, която позволява на купувача да може да проследи активността на акаунта и осъществените сесии. Ако потребителят разпознае нетипична активност, той може да информира администратора на платформата или да актуализира своите защити за вписване и възстановяване на информация. Потребителят може да използва своя акаунт при даден търговец еднократно за конкретна сделка или за ограничен брой сделки и от даден момент повече да не желае да осъществява покупки от същия агент на обмена. При това положение и съгласно чл. 17 на Регламент (ЕС) 2016/679 клиентът има право „да бъде забравен“, тази повелителна разпоредба става задължителна и трябва да бъде директно имплементиран в стопанския и обществения живот на всички държави–членки от 25 май 2018 г. Съгласно него, потребителят може да „поиска от администратора изтриване на свързаните с него лични данни без ненужно забавяне, тъй като те повече не са необходими за целите, за които са били събрани“ (Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета на Европа, 2016). Така всеки агент на обмена е обвързан със задължението да разработи задължителни фирмени правила за ефективна и законосъобразна защита на личните данни на европейските граждани, които събира и използва в своята бизнес дейност, независимо от това къде по света е регистрирана неговата компания. Това поставя в центъра интереса за защита на европейския потребител и невъзможността той да бъде заобиколен.

• Онлайн потребителят следва да полага грижа и да модернизира защитата на операционната система на използваната компютърна конфигурация най-малко чрез подходящ софтуер за противодействие от нежелани и вредни програми. Поддържането на използвания защитен софтуер в най-актуално състояние и версия на библиотеките за разпознаване на

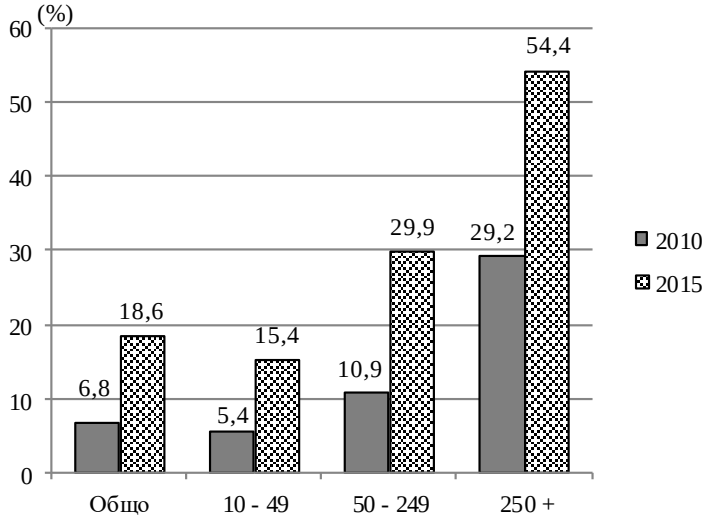
зловредните инструменти може да предотврати до определено ниво опасните въздействия. Това предполага да се поддържа и в най-актуална версия или издание използваната програма за преглед на съдържание в интернет. Едновременно с това културата и познанието на потребителя за услугите на информационното общество трябва да бъдат системно развивани, за да посрещат предизвикателствата на непрекъснатата дигитална трансформация и еволюция.

В тази връзка са изведени и препоръките на Европейския платежен съвет за ефективен контрол и облекчаване на последиците от заплахите в областта на плащанията, които се обобщават в ежегодни годишни доклади. Основните констатации в сферата на заплахите при електронни плащания са свързани с: „нарастващ професионализъм на киберпрестъпниците; увеличаващ се брой на атаките от типа за отказ на услуга (Distributed Denial of Service (D)DoS) и тяхната насоченост към финансовия сектор; промяна във фокуса на атаките от зловреден софтуер към тези на социалното инженерство; изменение при атакуваните сегменти от клиенти, търговци на дребно, малки и средни предприятия към ръководители на компании, служители, финансови институции и платежни инфраструктури; основната заплаха продължава да бъде на зловредния софтуер и по-специално рансъмуерът (софтуер за похищаване на компютърни системи и изнудване на техните собственици); разрастващи се ботнет мрежи, обусловено от значителния обем заразени потребителски устройства; многовекторни атаки и основно към финансови институции; растяща атрактивност към нападение на мобилни устройства и такива за интернет на нещата; адаптирането на облачни услуги и технологии за анализ на големи данни, води до повсеместно съхранение на данни, което създава нови възможности за бизнеса, но носи и нови рискове“ (European Payments Council, 2017, p. 5). Едно ново явление, което се появява, е „киберпрестъпността като услуга“ (European Payments Council, 2018, p. 6), което позволява да се развие алтернативен пазар на подобен род злонамерени услуги със свое специфично и високо профилирано търсене и предлагане.

Извън посоченото до момента по отношение на измамите при електронни разплащания в интернет следва да бъде упоменато и съществуването на значителен информационен проблем. Той засяга едновременно всички участници на безналичните платежни системи, поради отсъствието на специфично познание за непрекъснато увеличаващите се разновидности на измамните схеми и новите форми на киберпрестъпността. Понякога част от установената информация в определен етап от развитието на криминалните случаи остава неоповестена, за да бъдат открити каналите на нейното разпространение, което дава възможност да се достигне до първоизточниците на злоумишлените действия. Това често пъти води до забавяне и на защитните реакции на засегнатите страни. Последното определя защо „гарантирането на сигурността на киберпространството е обща отговорност“ (Европейска Комисия, 2013, стр. 9), в която ролята на

крайните потребители е основополагаща за постигане на по-безопасни електронни разплащания. Това означава изграждане на умения и компетенции за култура на електронни разплащания на всички потребители и участници на информационното общество.

Посочените аспекти дават възможностите на потребителското измерение на защита в реална и виртуална среда. От друга страна, бизнес агентите също могат да прилагат инструменти и политики за информационна сигурност. Според данните от репрезентативното изследване на българските предприятия за прилагане в тяхната дейност на информационните и комуникационните технологии през 2010 г., едва 6,8% от фирмите в страната имат официална политика за информационна сигурност (вж. фиг. 1) (ИНФОСТАТ - Национален статистически институт, 2018). След 5 години през 2015 г. почти една от 5 компании (18,6%) разполага с формализиран подход за ефективна защита на чувствителната информация. Въпреки отчетеното нарастване от над 274% разпространението на политиките за информационна сигурност все още е далеч от например средното равнище на ЕС-28, което е в размер на 28% за 2015 г. (Eurostat, 2018). В структурно отношение този процес е значително по-напреднал в големите икономически субекти с над 250 бр. заети лица, където повече от половината предприятия или 54,5% имат развита официална политика за информационна сигурност. Закономерно най-изоставащи в този процес са малките стопански единици с между 10 и 49 бр. заети лица, при които само 5,4% през 2010 г., а през 2015 г. 15,4% от тази подгрупа са предприели действия за управление на информационната сигурност във фирмата.



Фигура 1. Предприятия в България, които имат официална политика за информационна сигурност през 2010 и 2015 г. (в %) Източник: НСИ (Използване на ИКТ от предприятията).

В бъдеще този процес ще претърпи сериозна промяна, предизвикана от задължителното прилагане на Регламент (ЕС) 2016/679, който засяга всички физически или юридически лица, които при осъществяване на своята икономическа дейност придобиват и извършват операции по обработване на лични данни на физически лица. Последното ще наложи и определяне на адекватни и съобразени с нормативната уредба политики за защита на личните данни и основно в измеренията на информационната сигурност. Този подход създава ясни рамки на ангажиментите и отговорностите в работата на лицата с достъп до лични данни, необходимите действия за адекватно нормативно синхронизиране и цялостно обезпечаване на обработването на лични данни в рамките на организациите и същевременно гарантира най-висока степен на защита на индивидуалните права на гражданите на ЕС.

Заключение

В настоящето не съществува универсален и всеобхватен подход за защита на потребителите срещу измами в търговията, но колкото по-добре си взаимодействат клиентът и агентът на обмена, толкова и възможностите за възникване на зловредни ситуации ще бъдат редуцирани. Допълнително потребителите не следва безусловно да разчитат на добросъвестното поведение на останалите участници в реална и електронна търговска среда, а да приемат своята отговорност по опазване на личните си данни, платежни инструменти и при използване на платежните услуги и разплащателни системи.

Използвани източници

Bernard, B., Johnson, H. H., Hodgson, H., Mills, L., Coates, S., Turner, H., и др. (2017). *Online fraud.* National Audit Office. London: National Audit Office Press Office.

Dalla, E. H., & Geeta, M. (2013). Cyber Crime – A Threat to Persons, Property, Government and Societies. *International Journal of Advanced Research in Computer Science and Software Engineering, 3*(5), 997-1002.

Ecommerce news. (29 06 2017 г.). *UK and France account for 73% of European card fraud. И*зтеглено на 30 01 2018 г. от Ecommerce News: https://ecommercenews.eu/uk-france-account-73-european-card-fraud/

European Payments Council. (2017). *2017 Payment Threats and Fraud Trends Report.* Brussels: Conseil Européen des Paiements AISBL.

European Payments Council. (2018). *2018 Payment Threats ans Fraud Trends Report.* Brussels: Conseil Européen des Paiements AISBL.

Eurostat. (2018). *Enterprises had a formally defined ICT security policy.* Изтеглено на 08 02 2018 г. от ICT usage in enterprises (isoc_e): http://ec.europa.eu/eurostat/data/database

Federal Bureau of Investigation. (2018). *Internet crime report 2017.* Internet Crime Complaint Center.

Gelbmann, M. (03 01 2018 г.). *Web Technologies of the Year 2017.* Изтеглено на 30 01 2018 г. от W3Techs: https://w3techs.com/blog/entry/web_technologies_of_the_year_2017 и https://w3techs.com/technologies/overview/ssl_certificate/all

Juniper Research. (2016). *Online payment fraud whitepaper 2016-2020.* Basingstoke, Hampshire, United Kingdom: Juniper.

Kratcoski, P., Dobovsek, B., & Edelbacher, M. (2015). *Corruption, Fraud, Organized Crime, and the Shadow Economy.* Boca Raton, FL: CRC Press.

Masterindex 2017. (03 2017 г.). *Pan-European e-commerce and new payment trends.* Изтеглено на 30 01 2018 г. от https://newsroom.mastercard.com/wp-content/uploads/2017/03/Masterindex-2017.pdf

Matsuo, T., & Colomo-Palacios, R. (2013). *Electronic business and marketing: New trends on its process and applications.* SCI 484, Springer – Verlag Berlin Heidelberg.

Miller, S., Marchini, K., & Pascual, A. (01 02 2017 г.). *2017 Identity Fraud: Securing the Connected Life.* Изтеглено на 29 01 2018 г. от dba as Javelin Strategy & Research: javelinstrategy.com

Perez, J. (22 01 2018 г.). *Mastercard establishes biometrics as the new normal for safer online shopping.* Изтеглено на 28 01 2018 г. от Mastercard Press Releases: https://newsroom.mastercard.com/eu/press-releases/mastercard-establishes-biometrics-as-the-new-normal-for-safer-online-shopping/

The National White Collar Crime Center, Bureau of Justice Assistance, Federal Bureau of Investigation. (2008). *Internet crime report 2007.* Cybercrime reported to IC3.

Гайдаров, И. (27 Юни 2018 г.). *Как да избегнем фишинг измами?* Изтеглено на 28 Януари 2019 г. от PC World: https://pcworld.bg/polezno/2018/06/27/3211156_Как да избегнем фишинг измами%3F/

ГДБОП-МВР. (2018). *Заплахи в Интернет.* Изтеглено на 31 01 2018 г. от Официален сайт за борба с компютърните престъпления: http://www.cybercrime.bg/bg/internet/

Директива (ЕС) 2015/2366 на Европейския парламент и на Съвета на Европейския съюз. (23 Декември 2015 г.). Директива (ЕС) 2015/2366 от 25 ноември 2015 година за платежните услуги във вътрешния пазар, за изменение на директиви 2002/65/ЕО, 2009/110/ЕО и 2013/36/ЕС и Регламент (ЕС) № 1093/2010 и за отмяна на Директива 2007/64/. *Официален вестник на Европейския съюз, OJ L 337*, 35-127.

Директива 1999/93/ЕО на Европейския Парламент и на Съвета на Европа. (19 01 2000 г.). Директива 1999/93/ЕО от 13 декември 1999 година относно правната рамка на Общността за електронните подписи (отменена). *Официален вестник на Европейския съюз, OJ L 13, Special edition in Bulgarian: Chapter 13, Volume 028*, стр. 12-20 с. 120-129.

Допълнителни разпоредби на Закона за платежните услуги и платежните системи. (2017). *Обн. ДВ. бр.23 от 27 Март 2009г., посл. изм. ДВ. бр.97 от 5 Декември 2017г*.

Европейска Комисия. (2013). *Съвместно съобщение до Европейския Парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите. Стратегия на Европейския съюз за киберсигурност. Отворено, безопасно и сигурно киберпространство.* Брюксел: EUR-Lex - 52013JC0001 - BG - Службата за публикации на ЕС.

Закон за българските лични документи (загл. изм. - ДВ, бр. 82 от 2009 г.). (2017). *Обн. ДВ, бр. 93 от 11 Август 1998 г., посл. изм. ДВ, бр. 97 от 5 Декември 2017 г*.

Закон за електронния документ и електронните удостоверителни услуги (загл. изм. - дв, бр. 85 от 2017 г.). (2017). *Обн. ДВ, бр. 34 от 6 Април 2001 г., посл. изм. и доп. ДВ, бр. 85 от 24 Октомври 2017 г.*

Закон за защита на потребителите. (2018). *Обн. ДВ, бр. 99 от 9 Декември 2005 г., посл. изм. ДВ, бр.7 от 19 Януари 2018 г*.

ИНФОСТАТ - Национален статистически институт. (2018). *Предприятия, които имат официална политика за информационна сигурност.* Изтеглено на 28 02 2018 г. от https://infostat.nsi.bg/infostat/pages/reports/query.jsf?x_2=1365

Министерство на труда и социалната политика. (2017). Наредба № 4 за документите, които са необходими за сключване на трудов договор. Издадена от министъра на труда и социалната политика. *Обн. ДВ, бр.44 от 25 Май 1993г., изм. и доп. ДВ, бр.99 от 12 Декември 2017г.*

Наказателен кодекс. (2017). *Обн. ДВ, бр. 26 от 2 Април 1968 г., посл. изм. и доп. ДВ, бр. 101 от 19 Декември 2017 г.*

Национален статистически институт. (8 Декември 2017 г.). *Проблеми, срещани при поръчки или покупки на стоки и услуги през интернет.* Изтеглено на 28 Януари 2019 г. от НСИ: http://www.nsi.bg/sites/default/files/files/data/timeseries/ICT_HH_1.2.4.xls

Национален статистически институт. (16 Юли 2018 г.). *Престъпления по глави от наказателния кодекс и някои видове престъпления и по изход на делата.* Изтеглено на 23 Януари 2019 г. от НСИ: http://www.nsi.bg/sites/default/files/files/data/timeseries/JST_1.3.xls

Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета на Европа. (04 05 2016 г.). Регламент (ЕС) 2016/679 от 27 април 2016 година относно защитата на физическите лица във връзка с обра-

ботването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните). *Официален вестник на Европейския съюз, OJ L 119*, стр. 1-88.

Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета на Европа. (28 08 2014 г.). Регламент (ЕС) № 910/2014 от 23 юли 2014 година относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО. *Официален вестник на Европейския съюз OJ L 257*, стр. 73-114.

Фоукс, Г. (11 Ноември 2016 г.). *Сравнение на VPN протоколи: PPTP – L2TP – OpenVPN – SSTP – IKEv2.* Изтеглено на 23 Януари 2019 г. от vpnMentor: https://bg.vpnmentor.com/blog/vpn-protocol-comparison-pptp-vs-l2tp-vs-openvpn-vs-sstp-vs-ikev2/

Стопанска академия „Д. А. Ценов” – Свищов
Университет за национално и световно стопанство – София
Икономически университет – Варна
Софийски университет „Св. Климент Охридски”
Нов български университет – София

ИКОНОМИКА 21

Междууниверситетско списание
Година IX, книга 1, 2019

СЪДЪРЖАНИЕ

ИКОНОМИКА 21
МЕЖДУУНИВЕРСИТЕТСКО СПИСАНИЕ

Дадено за печат на 19.04.2019 г., излязло от печат на 11.06.2019 г., формат 70x100/16, тираж 70.

ISSN 1314-3123 (Print)
ISSN 2534-9457 (Online)

ISSN 2534-9457 (Online)
ISSN 1314-3123 (Print)

ИКОНОМИКА 21

Година IX, книга 1, 2019

- 10-те „НЕ” за мениджърска ефективност
- Инфраструктурни такси във въздушния транспорт – проблеми и проекции
- Защита срещу измамите при електронните разплащания в търговията

МЕЖДУУНИВЕРСИТЕТСКО СПИСАНИЕ

Economics 21
Year IX, Book 1, 2019
Година IX, книга 1 2019
Икономика 21

КЪМ ЧИТАТЕЛИТЕ И АВТОРИТЕ НА СПИСАНИЕ „ИКОНОМИКА 21"

Списание „Икономика 21" **публикува изследователски студии и статии, методологически и методически разработки.**

1. Обем:
Студии: минимум - 26 страници; максимум - 40 страници;
Статии: минимум - 12 страници; максимум - 25 страници;
Методологически и методически разработки до 40 страници.

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

3. Технически характеристики:
- изпълнение Word 2003 (минимум);
- размер на страницата - A4, 29-31 реда и 60-65 знака на ред;
- разстояние между редовете Single;
- шрифт - Times New Roman 12 pt;
- полета - Top - 2.54 см.; Bottom - 2.54 см; Left - 3.17 см; Right - 3.17 см;
- номерация на страницата - долу вдясно;
- текст под линия - размер 10 pt;
- графики и фигури - Word 2003 или Power Point.

4. Оформление:
- наименование на статията, име на автора, научна степен, научно звание - шрифт Times New Roman, 12 pt, с големи букви Bold - центрирано;
- наименование и адрес на месторабoтата; телефони за контакти и E-mail;
- резюме на български език в обем до 15 реда; ключови думи - от 3 до 5;
- **JEL** класификация на публикациите с икономически характер (http://ideas.repec.org/j/index.html);
- основен текст (изложение);
- таблиците, графиките и фигурите се вграждат софтуерно в текста (да позволяват езикова корекция и превод на английски);
- формулите се създават с Equation Editor;
- списък с цитираната литература, подреден по азбучен ред - на кирилица и на латиница;
- шаблон с технически характеристики и оформление - изтеглете оттук: https://www.uni-svishtov.bg/samagazine/upload/Economics-21-Template_bg.doc

5. Правила за цитиране под линия:
За библиографско цитиране на информационни източници се използва **APA Style**.
Неговите изисквания са поместени тук: https://www.uni-svishtov.bg/default.asp?page=page&id=71 и тук: http://www.apastyle.org/.
Всеки автор носи отговорност за отстояваните идеи, съдържанието и техническото оформление на своя текст.

6. Контакти:
Главен редактор: тел.: (++359) 631-66-338
Стилов редактор и ПР: тел.: (++359) 631-66-335
E-mail: i.varbanov@uni-svishtov.bg, economics21@uni-svishtov.bg
Адрес: Стопанска академия „Д. А. Ценов", ул. „Е. Чакъров" № 2, Свищов, България