УНИВЕРСИТЕТ ЗА НАЦИОНАЛНО И СВЕТОВНО СТОПАНСТВО

Катедра „Национална и регионална сигурност”

ПОДОБРЯВАНЕ НА КИБЕРСИГУРНОСТТА В МАЛКИЯ И СРЕДЕН БИЗНЕС В БЪЛГАРИЯ

АВТОРЕФЕРАТ НА ДИСЕРТАЦИОНЕН ТРУД ЗА ПРИСЪЖДАНЕ НА ОБРАЗОВАТЕЛНА И НАУЧНА СТЕПЕН „ДОКТОР" по научна специалност „Икономика и управление“ (Икономика на отбраната и сигурността), професионално направление 3.8. Икономика

Автор: Ивайло Христосков Илиев

Катедра: „Национална и регионална сигурност”

Научен ръководител: доц. д-р Нончо Иванов Димитров

Катедра: „Национална и регионална сигурност”

София, 2025 г.

Дисертационният труд е обсъден и насочен за защита от катедра „Национална и регионална сигурност“ при Университет за национално и световно стопанство – София.

Авторът на дисертационния труд е докторант на самостоятелна подготовка към същата катедра. Изследванията и разработките представени в дисертационния труд са извършени в Университет за национално и световно стопанство – София.

Дисертационният труд е с обем от 222 стандартни страници и съдържа: списък със съкращенията, списък с графиките и таблиците, увод, изложение в три глави, заключение, списък с приносите, списък с използвана литература и приложения.

Публичната защита на дисертационния труд ще се състои на 25.11.2025г. в зала „Научни съвети“ на УНСС – София, на открито заседание на Научното жури, назначено със заповед на Ректора на УНСС.

Материалите по защитата са на разположение на заинтересованите лица в дирекция „Наука“ на УНСС – София и на интернет страницата на Университета (www.unwe.bg)

I. ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

Актуалност на темата

Малките и средни предприятия в България са повече от 95% от всички икономически субекти – това прави този тип бизнес "гръбначният стълб" на родното стопанство. Тази метафора обаче, предвид мащабите, съвсем не е достатъчна. Нещо повече – малкият и среден бизнес представлява не само целия скелет, а и жизнените органи на българската икономика.

Предприемаческият климат у нас обаче, наред с редица други затруднения – финансови, институционални, културни – не осигуряват на този тип предприятия възможностите за спокойно развитие и необходимата защита. Докато някои от другите опасности обаче могат много лесно да бъдат преодолени, приети или управлявани, то тази от киберпрестъпления не е сред тях.

Дигитализацията на бизнеса се считаше за сила и преди пандемията от Covid-19. Ограниченията, породени от необходимостта от борба с вируса обаче пренесоха скорострелно по-голямата част от живота, и личен, и служебен, онлайн. Това, в съчетание с недостатъчната подготвеност както на потребителите (физически и юридически лица) в Интернет, така и на институциите в България, води до значително увеличаване на киберпрестъпността. Нейни жертви вече са все по-често обикновени граждани или малки бизнеси, а не цели институции или големи предприятия.

Това съвсем не е изненада – онлайн и мобилната търговия, интернет разплащанията, безкасовите плащания са вече начин на живот не само за отделни единици или за младите хора. Профилите в социалните мрежи и корпоративният уебсайт са основни инструменти за комуникация, които вече са дори в учебниците по маркетинг. Дигиталният маркетинг се откроява като една от най-желаните специалности за обучение и квалификация, а онлайн услугите спестяват на бизнеса време и пари.

Всичко това обаче изисква и целенасочени действия във връзка с ограничаването на вредните влияния на киберпрестъпленията. Необходимо е компаниите да предпазят както

собствените си служители и чувствителна информация, така и данните на клиентите и потребителите си. За това обаче имат нужда от проактивното съдействие и на двете страни – компетентните институции и самите потребители. Това означава висока институционална ефективност и поне средно ниво на култура на потребление, за съжаление и двете липсващи в България.

II. ОБЕМ И СТРУКТУРА НА ДИСЕРТАЦИОННИЯ ТРУД

Дисертационният труд е с обем от 222 стандартни страници и съдържа: списък със съкращенията, списък с графиките и таблиците, увод, изложение в три глави, заключение, списък с приносите, списък с използвана литература и приложения. Библиографията се състои от 198 литературни източника.

Дисертационният труд е структуриран в следната последователност:

СПИСЪК СЪС СЪКРАЩЕНИЯТА
СПИСЪК С ГРАФИКИТЕ И ТАБЛИЦИТЕ
УВОД
ПЪРВА ГЛАВА - СЪЩНОСТ И ПРОБЛЕМИ НА КИБЕРСИГУРНОСТТА В БЪЛГАРИЯ. ИЗМЕРЕНИЯ НА ДИГИТАЛИЗАЦИЯТА НА МАЛКИЯ И СРЕДЕН БИЗНЕС В БЪЛГАРИЯ
1.1 Теоретични измерения на киберсигурността. Понятиен апарат.
1.2 Фактори за увеличаване значението на киберсигурността в България
1.3 Малки и средни предприятия в България
1.4 Дигитализацията на малкия и среден бизнес в България
ВТОРА ГЛАВА - МЕТОДИКА ЗА ПОВИШАВАНЕ НА КИБЕРСИГУРНОСТТА В МАЛКИЯ И СРЕДЕН БИЗНЕС В БЪЛГАРИЯ
2.1 Първи етап – идентифициране и управление на рисковете за малкия и среден бизнес в България, свързани с дигитализацията
2.2 Втори етап – законодателни инициативи в подкрепа на киберсигурността

III. СЪДЪРЖАНИЕ И РЕЗУЛТАТИ ОТ ИЗСЛЕДВАНЕТО

УВОД

Киберсигурността се превръща в нарастващ проблем за малкия и среден бизнес в световен мащаб – все повече и повече атаки се извършват от престъпници, които се насочват към предприятията заради ценната информация, с която те разполагат, с единствената цел данните да бъдат продадени за големи суми на черния пазар.

Големите организации, разбира се, не са застраховани. Те обаче разполагат със значително по-големи финансови, човешки, технологични ресурси, което може да им бъде от полза тогава, когато се налага бързо да бъдат ограничени последиците от кибератаките. По-малкият ресурс, с който работят, включително и от гледна точка на масиви от данни и чувствителна информация, обаче не води до по-добра защита на малките и средни компании, нито отклонява интереса на престъпниците от тях.

Тревожни данни на Форбс показват, че киберпрестъпленията се увеличават шест пъти по време на пандемията. Никой, нито дори известните личности, не са застраховани – нещо повече, през 2020 г. са компрометирани 130 Twitter профила, сред които тези на Елън Мъск и Барак Обама. През същата година хотелската верига Marriott претърпява кибератака, по време на която изтичат данните на повече от 300 млн. гости на хотелите.

Видно е, че въпреки огромните ресурси за защита дори технологичните гиганти не успяват да се справят с киберпрестъпността. Малките предприятия, особено в развиващи се икономики с редица други проблеми, стават още по-уязвими на атаки. Те в повечето случаи нямат технологичните защити, необходими за предпазване от атаки, не разполагат и с необходимите ресурси, за да вложат сериозно в киберсигурността.

Логиката на извършителите вероятно се крие в това, че малките размери на бизнеса не означават и също такова ограничение във финансов или ресурсен аспект – тоест, малкият бизнес може да работи с големи суми пари и количество клиентски данни точно толкова, колкото и големият, но е по-слабо защитен. Наистина по-голямата част от малкия и среден бизнес у нас няма никакъв план или технология за защита на киберсигурността – така тези предприятия се превръщат в удобна цел.

Нещо повече, може да се окаже, че заплахите за киберсигурността на малките и средни предприятия идват дори отвътре, при това не поради злонамереност, а поради недостатъчна квалификация и неусвоени (понякога генерално) умения за засичане и противодействие на кибератаки. За съжаление, често това е валидно не само за редовите служители (ако има такива), а и за самите собственици и управители на малките бизнеси.

Ransomware атаките са сред най-разпространените заплахи за киберсигурността, пред които са изправени малките предприятия днес. Тук става дума за криптиране данните на компанията и държането им “като заложник”, докато не бъде платен откуп. На тези атаки рядко се обръща внимание преди да е станало късно – обикновено те се случват по имейл, чрез линк към обикновен документ. Тъй като дори при едно микропредприятие обемът на електронна комуникация може да е значителен, повечето хора разбират грешката си едва след като са отворили криптиращия файл. След това в повечето случаи плащат “откупа”, дори и той да им струва няколко хиляди лева, защото нямат времето и ресурсите да

възстановят криптираната информация или се опитват да спестят от ползване на качествен backup като част от нормалния си протокол за работа.

Фишингът пък е несъмнено най-голямата и популярна кибер заплаха, пред която са изправени малките и средни предприятия. Тези атаки работят, като подмамват потребителя да предостави личната си информация чрез изпращане на имейл, който изглежда като от доверен източник или уебсайт. Никоя компания, независимо от размера си, не е "имунизирана" срещу тези измами. Примерите от българската действителност тук са много, но в повечето случаи са свързани със социалните мрежи и/или банкова информация, която се изисква по имейл в прозорец, който представлява много точно копие на истинския. Едва след като се е случил инцидентът, при връщане назад и по-внимателно вглеждане измамеият разбира грешката си.

Друг сравнително прост метод за атака на малките предприятия е злонамереният софтуер. Атаките от този тип работят чрез проникване в компютър чрез прикачен файл към имейл или друга вратичка и след това се изпълняват без знанието на потребителя. Веднъж попаднал вътре, злонамереният софтуер може да причини хаос в цифровите файлове, като промени настройките и разрешенията, блокира изпълнението на конкретни програми и шпионира активността на потребителите. Зловреден софтуер често се среща и в обществени Wi-Fi мрежи, където потребителите са изложени на риск устройствата им да бъдат компрометирани, ако посетят заразен уебсайт или просто преглеждат грешната страница.

Социалното инженерство пък е техника, чрез която престъпниците подмамват хората да предоставят чувствителна информация чрез различни средства – представят се за някой друг, най-често представител на компания-потенциален партньор или контрагент. С нарастването на популярността на социалните мрежи, социалното инженерство става все по-широко разпространено и съобщенията, изпратени чрез тези платформи, може да съдържат зловреден софтуер, който пък може да открадне личната информация на потребителя.

Една от основните тревоги за малкия и среден бизнес е именно кражбата на данни. Това престъпление се случва, когато хакерите вземат лична информация от служители чрез измама или нечестни практики. Получавайки достъп до имейл акаунта на служител,

хакерите могат лесно да разпространяват рансъмуер, фишинг и фарминг атаки в мрежата на компанията.

Самите служители често представляват значителна заплаха за сигурността на бизнеса от всякакъв размер. Те оставят данни на USB устройства, осигуряват лесен достъп до фирмени файлове, като използват една и съща парола както за лични, така и за служебни акаунти и попадат на фишинг схеми, които ги подмамват да предоставят информацията си за вход. Така много често се оказва, че пробивите в киберсигурността на малките и средни предприяти се оказват плод на човешка грешка, дори не на злонамерени действия.

Този кратък преглед на най-често срещаните примери за киберпрестъпления срещу малкия и среден бизнес и акцентирането върху някои техни особености идва да покаже, че предотвратяването на атаки чрез целенасочени мерки е най-добрият вариант. Най-добрият начин малките предприятия да се защитят от киберпрестъпления е да имат завършен план за сигурност – такъв, който включва предотвратяване на загуба на данни, въведен план за реагиране при инцидент, преглед на привилегиите за достъп на персонала и обучение на служителите относно най-добрите практики за киберсигурност.

И във връзка с горепосоченото можем да посочим, че основният изследователски проблем, който дисертационният труд разглежда, е киберсигурността на малкия и среден бизнес в България и необходимостта от координирани действия за нейното повишаване.

Така се стига и до обекта на изследване на дисертационния труд, а именно конкретните проблеми на киберсигурността, с които се сблъсква малкия и среден бизнес в България. Предмет на изследване пък е именно повишаването и превенцията прилагаща се в малките и средни предприятия у нас.

В дисертацията са използвани следните методи: анализ на литературни и информационни източници, проучване на чуждия опит, качествен анализ на риска, сравнителен анализ, казусен анализ и емпирично изследване и проучване на нагласите и разбиранията по отношение на киберпрестъпността и киберсигурността от страна на потребителите и на собствениците и ръководителите на малък и среден бизнес.

Цел на дисертацията е да се очертаят ясно измеренията на проблемите на киберсигурността на малкия и среден бизнес у нас заедно с техните взаимовръзки с институциите и клиентите и да се дадат препоръки за подобряването на ситуацията за българските компании. В този смисъл могат да бъдат формулирани следните задачи:

- да се изгради теоретична и нормативна рамка и да се направи анализ на киберпрестъпността;
- да се разработят методически решения и да се представят добри практики;
- да се проведе емпирично изследване за измерване за нагласите и степента на разбиране на проблемите, свързани с киберсигурността, както у потребителите, така и у собствениците и ръководителите на малки и средни предприятия;
- да се дадат конкретни препоръки за подобряване на киберсигурността и бизнес климата в България, базирани на резултатите от емпиричното изследване и разработените методически решения.

Основната теза, която ще се защитава в дисертацията е, че в България, повече отколкото в по-добре развитите западноевропейски икономики, киберсигурността на малкия и среден бизнес е проблем, който изисква незабавни координирани действия от страна на институции, предприятия и потребители. Именно липсата им към момента влошава бизнес климата и пречи на изграждането на трайни взаимоотношения на доверие между компании и клиенти в момента.

В подкрепа на това твърдение са използвани редица **литературни и информационни източници –** тук се нареждат специализирана литература по темата, статистически данни от НСИ, Евростат, институционална статистика и изявления, онлайн и офлайн публикации на експерти по темата.

Поставените **ограничения** са свързани с териториалния обхват и долимината на бизнеса. Изследването е базирано и фокусирано на държавните територии на Република България. Изследването е ограничено и до малък и среден бизнес и специфичния български контекст. Това обстоятелство може да ограничи пряката приложимост на резултатите и

разработената методика към големи корпорации или към МСП в държави с драстично различна нормативна база, институционална среда и култура на киберсигурност.

Потребители на резултатите и разработената методика за повишаване на киберсигурността на МСП в България биха били полезни за няколко ключови групи. Основната целева група са собствениците и ръководителите на малки и средни предприятия, които могат да използват методиката за оценка, планиране и въвеждане на адекватни мерки за киберзащита в техните компании, като по този начин намалят риска от финансови и репутационни щети. Държавните институции и регулаторните органи, като например Министерството на електронното управление, също са важен потребител, тъй като дисертацията разглежда нормативната база и призовава за координирани действия; те могат да използват препоръките за подобряване на политиките за киберсигурност, програми за подкрепа и информационни кампании, насочени към малкия бизнес. Организациите за подкрепа на бизнеса (като браншови камари и асоциации) могат да включат резултатите от изследването в обучителни програми, семинари и консултации, които предоставят на своите членове. Освен това, консултантски компании и доставчици на услуги по киберсигурност могат да използват методиката и данните от емпиричното проучване за адаптиране и подобряване на своите продукти и услуги, предлагани на МСП. Накрая, академичната общност може да използва дисертацията като теоретична и емпирична основа за бъдещи изследвания в областта на киберсигурността, икономиката и електронното управление в България.

ПЪРВА ГЛАВА - СЪЩНОСТ И ПРОБЛЕМИ НА КИБЕРСИГУРНОСТТА В БЪЛГАРИЯ. ИЗМЕРЕНИЯ НА ДИГИТАЛИЗАЦИЯТА НА МАЛКИЯ И СРЕДЕН БИЗНЕС В БЪЛГАРИЯ

1.1 Теоретични измерения на киберсигурността. Понятиен апарат.

Терминът „киберсигурност“ е предмет на редица академични и популярни трудове, които до голяма степен разглеждат темата от определена гледна точка. Понятието се използва широко и неговите определения са силно променливи, обвързани с контекста, често субективни и понякога неинформативни. Има малко литература за това какво

всъщност означава киберсигурност и как е разположен феноменът в различни контексти. Липсата на кратка, широко приемлива дефиниция, която да улавя многоизмерността на киберсигурността, потенциално възпрепятства технологичния и научен напредък, като засилва предимно техническия възглед, същевременно разделяйки дисциплините, които трябва да действат съгласувано за разрешаване на сложни предизвикателства пред киберсигурността. Например, има спектър от технически решения, които поддържат киберсигурността – въпреки това, тези решения сами по себе си не се справят с проблема. Има множество примери и значителна научна работа, които демонстрират предизвикателствата, свързани с организационните, икономическите, социалните, политическите и други човешки измерения, които са неразривно свързани с усилията за киберсигурност[1]. Фредрик Чанг, бивш директор по изследванията в Агенцията за национална сигурност в Съединените щати, обсъжда интердисциплинарния характер на киберсигурността:

1.2 „*Науката за киберсигурността предлага много възможности за напредък въз основа на мултидисциплинарен подход, защото в края на краищата киберсигурността е основно свързана със съперничество. Хората трябва да защитават машини, които са атакувани от други хора, използващи машини. Така че, в допълнение към критичните традиционни области на компютърните науки, електроинженерството и математиката, са необходими перспективи от други области*."[2]

1.3 Кавълти отбелязва, че има множество взаимосвързани дискурси около областта на киберсигурността[3]. Деконструирането на термина киберсигурност помага да се постави дискусията в двете области на „кибер" и „сигурност" и разкрива някои от наследените проблеми. „Кибер" е префикс, означаващ киберпространство и се отнася до електронни комуникационни мрежи и виртуална реалност[4]. Той еволюира от термина

[1] Goodall, J. R., Lutters, W. G., & Komlodi, A. 2009. Developing Expertise for Network Intrusion Detection. Information Technology & People, 22(2): 92-108.

http://dx.doi.org/10.1108/09593840910962186 последно посетен на 22.01.2024

[2] Chang, F. R. 2012. Guest Editor's Column. The Next Wave, 19(4): 1–2.

[3] Cavelty, M. D. 2010. Cyber-Security. In J. P. Burgess (Ed.), The Routledge Handbook of New Security Studies: 154-162. London: Routledge.

[4] Oxford University Press. 2014. Oxford Online Dictionary. Oxford: Oxford University Press. October 1, 2014:

"кибернетика", който се отнася до "*областта на теорията за контрол и комуникация, независимо дали в машина или в животно*"[5].

Изправени пред много дефиниции на киберсигурността от литературата, анализаторите е необходимо да следват прагматичен качествен изследователски подход в подкрепа на процеса на дефиниране, който обединява обективно качествено изследване със субективно качествено изследване . Всъщност резултатът трябва да бъде условно определение, което се основава на обективност (напр. система за откриване на проникване) срещу предположение (напр. намеренията на хакер).

Липсата на кратка, универсално приемлива дефиниция, която да обхваща многоизмерността на киберсигурността, възпрепятства технологичния и научен напредък, като засилва предимно техническия възглед за киберсигурността, като същевременно разделя дисциплините, които трябва да действат съгласувано, за да разрешат сложни предизвикателства пред киберсигурността. Става все по-очевидно, че киберсигурността е интердисциплинарно явление. По-обхватното, обединяващо определение, има за цел да улесни интердисциплинарните подходи към киберсигурността – една такава дефиниция следва да бъде възприета от множеството дисциплини, ангажирани с усилията за киберсигурност, като по този начин може да се постигне по-добро разбиране и сътрудничество, необходими за справяне с нарастващите и сложни заплахи за киберпространството и системите, активирани от киберпространството.

1.2 Фактори за увеличаване значението на киберсигурността в България

Компютърните и информационните системи революционизират механизма за обслужване по целия свят. Услугите, предлагани на индивида и общността ръчно, изчезват в полза на онлайн услугите с използването на компютърни и интернет технологии. Електронното обучение, електронната търговия, електронният бизнес, а в последно време и електронното правителство трансформират традиционните начини за работа във виртуален свят, където общуването “лице в лице” се случва, без да сте лице в лице. Иновациите, диференциацията в разходите и растежа, съюзите и сливанията са днешните

http://www.oxforddictionaries.com/definition/english/Cybersecurity последно посетен на 22.01.2024

[5] Wallinger, W., Alderson, D., & Doyle, J. 2009. Mathematics and the Internet: A Source of Enormous Confusion and Great Potential. Notices of the American Mathematical Society, 56(5): 586-599.

характеристики на организациите, които са възможни благодарение на цифровата революция[6]. Въпреки всички положителни страни и възможности, които дигитализацията предлага най-вече на малкия и среден бизнес, активното използване на новите технологии е свързано не само със социален напредък, но, особено в развиващите се икономики, поставя на дневен ред и въпроса за киберсигурността и увеличаващата се киберпрестъпност. Опасностите в Мрежата са една от основните причини редица МСП в развиващите се страни все ще да се чувстват неуверени по отношение на присъединяването към онлайн общността, което обяснява и по-ниските нива на дигитализация на частния и публичния сектор в тези икономики.

Трябва да се има предвид, че киберпрестъпността е престъпна дейност, чийто източник е компютър или компютърна мрежа, използвана за кибератаки, и може да включва измама, кражба, изнудване, фалшифициране и злоупотреба, но поради виртуалния режим е известно, че е трудно да се открие и наказват поради техническа сложност и невидимост нападатели, които седят на хиляди километри. Въпреки че новите технологии са удобни, динамични и развиващи се и всяко следващо тяхно ниво усъвършенства функции и механизъм за сигурност, поради естеството на киберпрестъпността и способността й да се развива с технологията, се появяват нови заплахи с тревожна степента на редовност. Така способностите на потребителите да си сътрудничат биват изправени пред все по-големи предизвикателства, което също може да застраши сигурността и финансовото здраве на всички МСП в Мрежата.

Проблемите, произтичащи от подобни престъпления, придобиват голямо значение, особено тези, свързани с кракване, нарушаване на авторски права, детска порнография. Те се наричат още проблеми с поверителността, когато хакери/нападатели атакуват поверителната информация, за да направят умишлени изкривявания, да откраднат и прихванат законно или по друг начин. Въпреки че съществува международна правна система, която се опитва да държи участниците отговорни за престъпни деяния чрез

[6] Madhava S.S.P., & Umarhathab, S. (Eds.), (2011). Information Technology Act and cyber terrorism: A critical review. Cyber Crime and Digital Disorder, Tirunelveli, India: Publications Division, Manonmaniam Sundaranar University.

Международния наказателен съд (МНС), липсата на координация или несъвместимостта на местните с международните закони се превръща в бариера пред нейния успех[7].

Онлайн комуникацията се е превърнала в норма в цифровата ера, поради което интернет потребителите и правителствата са изправени пред повишен риск да станат жертви на кибератаки. Киберпрестъпниците непрекъснато развиват авангардни техники, като изместват целите си, фокусирайки се по-малко върху кражба на финансова информация и повече върху бизнес шпионаж и достъп до правителствена информация. В контекста на бързо разпространяващите се киберпрестъпления правителствата в развиващите се страни трябва да си сътрудничат в световен мащаб, за да може да се разработи ефективен модел за контрол на заплахите. Благодарение на развитието и напредъка в компютърните и телекомуникационните технологии, развиващите се страни са в състояние да развият и разширят своите комуникационни мрежи, като им позволят по-бързо и по-лесно свързване в мрежа и обмен на информация. С това киберпрестъпленията се увеличават през последните няколко години в световен мащаб, което драматично промени сценария – в наши дни престъпниците използват по-сложни устройства, за да пробият киберсигурността. Нещо повече, в последните години зловреден софтуер, спам имейли, хакване на корпоративни сайтове и други атаки от този характер са дело на компютърни „гении“, очевидни от техния талант.

Тези рядко злонамерени атаки постепенно са се превърнали в синдикати за киберпрестъпления, източващи пари чрез незаконни киберканали. Според оценки само преди десетилетие около 2 милиарда потребители на интернет и 5 милиарда мобилни телефони са свързани по света. Всеки ден се обменят около 294 милиарда имейла и 5 милиарда телефонни съобщения[8]. Удобството на цифровите мрежи обаче има цена, тъй като бизнес организациите в частност и обществата като цяло все повече разчитат на компютрите и интернет базираните мрежи, поради което киберпрестъпността и цифровите атаки са се увеличили многократно по целия свят. Атаките са категоризирани като финансови измами, компютърно хакване, изтегляне на порнографски изображения от

[7] Grabosky, P.N., Smith, R.G., & Dempsey, G. (2001). Electronic theft: Unlawful acquisition in cyberspace, Cambridge University Press, Cambridge

[8] Zinnbaur, D. (2005). Internet governance priorities and practices, United Nations

интернет, вирусни атаки, преследване на електронна поща и създаване на уебсайтове, които насърчават расова омраза[9]. Основната и водеща стъпка към защита е по-доброто разбиране на различните видове заплахи, пред които са изправени бизнес общността и онлайн потребителите.

Често срещаните киберпрестъпления включват измами с предварителна такса, обяснение на ботнет мрежи, отказ от услуга (DoS) и разпределен отказ от услуга (DDoS), измами с подновяване на имена на домейни, фалшиви реклами, хактивизъм, кражба на лаптоп или друг хардуер, кражба на самоличност, IP кражба, копиране на информация, фишинг, софтуер за страхуване, социални медии, спам, шпионски софтуер, незащитени безжични локални мрежи (WLAN) и вирусни атаки[10]. Експертите са на мнение, че някои правителствени агенции може също да използват кибератаки вместо въоръжена война като ново средство за водене на война и това беше съобщено през 2010 г., когато Stuxnet (компютърен вирус) е използван за извършване на невидима атака на Иранската ядрена програма, която трябваше да деактивира иранските центрофуги за обогатяване на уран. Carders Stealing Bank, която също е известна като данни за кредитна карта, също е голямо киберпрестъпление, при което дублирани карти се използват за теглене на пари в брой от банкомати или в магазини[11].

Имайки предвид международния характер на киберпрестъпността, тя може да се случи не само в регионите, откъдето произхожда, а да включва и други държави или региони. Следователно киберпрестъпността се нуждае не само от силно реагиращи, но и от международно координирани мерки за контрол. По същия начин механизмът за разследване и докладване на тези престъпления трябва да изисква много ресурси.

Киберпрестъпниците и техните техники непрекъснато се променят, което изправя правителствата и бизнеса пред голямото предизвикателство да бъдат в крак с постоянното развитие на нарушителите. Според Роб Уейнрайт, директор на Европол, криминални

[9] . Herhalt, J. (2011). Cyber-crime-A growing challenge for governments, KPMG Issues Monitor, 8: 1-24, https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-crime.pdf последно посетен на 23.01.2024

[10]KPMG (2013). Global eFr@ud Survey, KPMG Forensic and Litigation Services.

[11] Chapman, A., & Smith, R.G. (2001). Controlling financial services frauds, Trends and Issues in Crime and Criminal Justice, 2: 189, Australian Institute of Criminology, Canberra

разследвания на киберпрестъпления, идентифицирането и проследяването на произхода на престъпността е не само сложно, но понякога и невъзможно поради безграничното си естество, което е едно от големите предизвикателства за развиващия се свят, който вече изпитва недостиг на технологии[12]. Редица експерти в различни части на света, че кибератаките и киберпрестъпленията са доходоносно начинание – в киберсвета хакерите извършват организирана престъпност, като продават поверителна откраднатa информация.

Експлоатацията чрез софтуер е често срещан начин, чрез който хакерите получават достъп до системи и чувствителна информация. Софтуерът за актуализиране на потребителите на свързани в мрежа машини също е лесен начин за киберпрестъпниците. По този начин актуалните инструменти и антивирусен софтуер могат да бъдат много полезни при защитата на мрежата и системите, използвани от онлайн потребителите, тъй като водещата антивирусна програма може да открива, премахва и защитава машините и мрежите на потребителя от зловреден софтуер и т.н. По същия начин, потребителите трябва да бъдат внимателни и да избягват пиратския софтуер. Образованието и грамотността могат да помогнат по-добре за предотвратяване на киберпрестъпленията, така че обучението за това как да бъдат използвани информационните системи и как да избягвате или да се предпазвате от престъпниците в киберпространството е необходимост, за да могат потребителите ясно да разбират най-често срещаните хакерски действия тактики, като фишинг, социално инженерство или подслушване на пакети и други[13]. Образованието и осведомеността в на онлайн потребителите трябва да изминат дълъг път, за да ги предпазят от много видове киберпрестъпления – въвеждането на нови технологии изисква обучение не само за използването на новите системи, но и за правата, задълженията и отговорностите, свързани с новите машини.

По подобен начин разпоредбите и законите, които управляват електронните системи, трябва да бъдат широко разпространени, така че потребителите да са наясно с регулаторните закони и мерки за киберпрестъпления, въведени от техните правителства,

[12] Council of Europe. (2003). Additional protocol to the convention on cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (ETS 189), http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm последно посетен на 23.01.2024

[13] . Herhalt, J. (2011). Cyber-crime-A growing challenge for governments, KPMG Issues Monitor, 8: 1-24,https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-crime.pdf последно посетен на 23.01.2024

както и в международен план. От друга страна, лошата и консервативна система за разследване също е пречка пред електронната сигурност, тъй като професионалната некомпетентност и политическата намеса в регистрацията на FIR, системата за разследване и тромавите процедури за забавяне в съдебната система на страната забавят правосъдието, като по този начин възпрепятстват правилното прилагане на кибер-законите. Друго средство за изкореняване на киберпрестъпността е хармонизирането на международното сътрудничество и законодателството – особено по отношение на мотивираните от алчност и кибертерористи[14].

По време на ограниченията поради разпространението на COVID-19 много малки предприятия трябваше спешно да преминат към дистанционна работа, отваряйки поради горепосочените причини възможности за възникването на много проблеми с киберсигурността, от работници, използващи персонални компютри за свързани с работата задачи, до разчитане на облака с малко или никакъв ИТ персонал или ресурси.

Киберпрестъпниците могат лесно да манипулират малкия бизнес – тези организации не могат да кажат „не“ на атаките с ransomware, тъй като нямат резервна система за възстановяване на данни, ако бъдат атакувани. Всичко това отново е свързано с ограниченията във финансовите средства, с които МСП са принудени да се справят.

Човешката грешка е водещата причина за злоупотребите с данни в малкия бизнес. Докладът на IBM също така установява, че компрометираните идентификационни данни са най-честият начин, по който киберпрестъпниците първоначално атакуват данните на компанията. Тъй като малките предприятия не се фокусират върху обучението по киберсигурност, често отново поради липса на финанси, служителите могат лесно да бъдат подмамени да попаднат на измами със социално инженерство, злонамерени заплахи или споделяне на данни за вход, чувствителни данни и друга фирмена и клиентска информация, тъй като не знаят какво да търсят, за да идентифицират подозрителни кибер дейност[15].

[14] . Herhalt, J. (2011). Cyber-crime-A growing challenge for governments, KPMG Issues Monitor, 8: 1-24,https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-crime.pdf последно посетен на 23.01.2024

[15] IBM, https://www.ibm.com/downloads/cas/OJDVQGRY последно посетен на 23.01.2024

Тъй като киберпрестъпността нараства и напредва с всяка изминала година, по-важно от всякога е малките предприятия да разберат как тези видове атаки могат да повлияят на операциите им и да предприемат правилните стъпки, за да се защитят. Ранното откриване на нарушение на данните е от решаващо значение за спасяването на репутацията на компанията и щети, възлизащи на хиляди, без самите практики да са изключително скъпи.

Най-добрите практики за киберсигурност на малкия бизнес включват:

●системно обучение на служителите – предприятията трябва да обмислят непрекъснато обучение, за да са добре запознати всичките им служители с потенциалните уязвимости в сигурността, за разпознаване и избягване на измами, създаване на силни пароли и защита на чувствителна информация за клиенти и компании;

●актуализиране на софтуера за сигурност – компаниите трябва да използват защитни стени, антивирусен софтуер и антишпионски програми, за да гарантират, че чувствителните данни не могат да бъдат лесно достъпни от хакери. Тези програми за сигурност също изискват редовни актуализации, за да предпазват успешно от уязвимости, така че мениджърите на МСП следва редовно да проверяват уебсайтовете на доставчиците на софтуер, за да научат за предстоящите корекции за сигурност и други актуализации;

●защита на фирмените данни – тъй като много злоупотреби се случват поради грешка на служителите, те следва да имат достъп само до жизненоважна информация за тяхната конкретна позиция. Компаниите трябва да обмислят програми за съхранение на записи, изискващи от служителите правилно да изчистват или архивират файлове. Редовното архивиране на данните на всички компютри и разполагането със система за възстановяване, ако информацията трябва да бъде извлечена поради кибератака със сигурност струват по-малко от откупа за криптиращия ключ. Сегментирането на мрежа е друг начин да избегнете споделяне на данни в цялата мрежа. По този начин, ако част от мрежата е компрометирана, не всичко е изчезнало поради сегментирането.

●политики за защита на парола – малките предприятия и техните служители трябва да използват силни пароли за всеки сайт, до който се влиза ежедневно. Паролите никога не трябва да се споделят между служители или да се записват, където другите могат да ги видят. Това е безплатна практика, която обаче може да спести на МСП много проблеми;

●шифроване на данни – всички данни, достъпни чрез лични устройства, компютри или сървъри трябва да бъдат защитени чрез подходящо криптиране в случай на опити за неоторизиран достъп. Когато данните са криптирани в покой, те са защитени от преглед, освен ако потребителят не разполага с правилните идентификационни данни и код. Това е много важно за всички регулирани от HIPAA данни;

●многофакторно удостоверяване – този инструмент изисква допълнителна информация за проверка, например код за сигурност, изпратен на вашия телефон, за влизане в мрежи, системи и компютри. Когато е възможно, е важно да се използва MFA. Включването му за имейл, VPN достъп, защитна стена и софтуерен достъп води до по-сигурна система и отново не струва допълнителни пари на компанията;

●киберзастрахователно покритие – киберзастраховането може значително да помогне за защитата на малкия бизнес от потенциалните екстремни разходи, които възникват от набор от кибератаки и финансовите щети и щетите за репутацията, причинени от пробиви на данни. Обработчиците на кибер искове са хората, които да насочват потърпевшите ръководители на малки бизнеси по време на стресиращия процес и да им помогнат да подберат доставчици, които са внимателно подбрани съгласно конкретните нужди и условия на предприятието.

Киберпрестъпниците често използват човешката уязвимост и психологически елементи, за да откраднат идентификационни данни и да получат неоторизиран достъп. Тъй като атаките с фишинг и социално инженерство са насочени предимно към хора, човешкият фактор продължава да бъде важен елемент, който CISO трябва да вземат предвид, за да защитят организациите си от кибератаки. Повечето злоупотреби с данни са причинени от човешка грешка, небрежност или липса на осведоменост, например чрез просто щракване върху грешна връзка. Така че е обичайно служителите да увеличават цифровия си отпечатък, без да са наясно с свързаните с това рискове.

„Хората са най-слабото звено в киберсигурността.“ – тази негативна характеристика на човешката природа е дълбоко вкоренена в индустрията за киберсигурност. В резултат на това има редица пречки пред това да има целенасочена, градивна дискусия как по-добре да се включат хората в процесите на киберсигурността. За разлика от технологиите и техническите процеси обаче хората са непостоянни и непредвидими. Проблемът с

човешкия фактор е сложен, защото по своята същност предполага сериозна социологическа, психологическа и философска дискусия[16].

В борбата срещу кибератаките човешката интуиция и креативност винаги ще бъдат решаващи. По време на геополитическо напрежение, например, анализаторите по сигурността могат да предвидят човешкото поведение, да предвидят престъпни дейности и да разберат защо заплахите се насочват към конкретни организации. Киберсигурността обаче не може и не трябва да бъде отговорност на един екип или отдел – тя трябва да бъде споделена отговорност в цялата организация, както и в нейната разширена екосистема от партньори, доставчици и клиенти.

Тъй като организациите възприемат хибридни модели на работа и ускоряват приемането на облака, те стават по-податливи на поглъщане на акаунти и други видове измами. Ето защо е важно служителите да разберат как кибератаките могат да повлияят на техния бизнес и как да се защитят от първия ден. Новите служители трябва да преминат обучение за осведоменост относно киберсигурността като част от процеса на набиране и адаптиране. Наред с това обучението за информираност относно сигурността трябва да бъде непрекъснат процес, който да обхваща голямо разнообразие от теми и примери за фишинг, ransomware и атаки чрез социално инженерство.

Въпреки че обучението по сигурността е полезно и задължително, служителите невинаги използват тези знания без стимул за това. Някои виждат геймификацията като потенциално средство за насърчаване на активно участие в дейности за киберсигурност, но това само по себе си няма да бъде ефективно, ако няма реални инструменти, които да го позволят. Съвременният пейзаж на киберсигурността е станал твърде широк и сложен, за да бъде разбран само от хората, така че използването на стратегия за защита в дълбочина може да се окаже от съществено значение. Чрез модернизиране и автоматизиране на ИТ

[16] Coventry, L., Briggs, P., Blythe, J., & Tran, M. (2014). Using behavioral insights to improve the public's use of cyber security best practices. Government Office for Science

процесите може би е възмостно да се намали и подобри въздействието на човешкия фактор върху киберсигурността[17].

Европейската комисия (2005 г.) дефинира значението на дефиницията на Европейския съюз за МСП по следния начин: В единен пазар без вътрешни граници, от съществено значение е мерките в полза на МСП да се основават на обща дефиниция, за да се подобри тяхната последователност и ефективност и да се ограничат нарушенията на конкуренцията. Това е още по-необходимо, като се има предвид широкото взаимодействие между националните мерки и мерките на ЕС за подпомагане на МСП в области като регионално развитие и финансиране на научни изследвания... За държавите-членки използването на определението е доброволно, но Комисията ги приканва, заедно с Европейската инвестиционна банка (ЕИБ) и Европейския инвестиционен фонд (ЕИФ) да го прилагат възможно най-широко. Въпреки обема на дефинициите на МСП, съществува тенденция да се приемат количествени критерии, на първо място критерия за броя на персонала или броя на служителите като основен определящ фактор при категоризирането на МСП. Също така в рамките на този компромис има тенденция за дефиниции, които се разпространяват отвъд границите на отделна държава във време, когато икономическото взаимодействие между страните е интензивно. Именно продукт на тези дефиниции е дефиницията за МСП, легитимирана от Европейския съюз и която се използва от повечето изследователи.

Икономическата литература съдържа големи разлики в дефиницията на малки и средни предприятия. Статистическите агенции, международните организации, правителствата на независими страни се появяват с различни дефиниции и категоризации за предприятията, които не отразяват разликите между тях. Различните определения на МСП са по-скоро произволни, отколкото приликата на нивото и естеството на икономическото развитие. Няма уникална, универсално приета дефиниция за малки и средни предприятия. Настоящите критерии са претърпели ревизия и винаги са в процес на оценка. Няма нито едно от двете съгласие, нито склонност към сближаване по отношение на дефинициите, дори между международни организации, които обединяват като членове

[17] Norris, G., Brookes, A., & Dowell, D. (2019). The psychology of internet fraud victimization: A systematic review. Journal of Police and Criminal Psychology, 34(3), 231–245

едни и същи държави. Значението на дефиницията на МСП за политиците се състои в оценяването на категориите предприятия и техния принос към заетостта, брутния вътрешен продукт и други макроикономически показатели, за насочване на усилията, политиките, стратегиите за развитие и програмите за подпомагане на малките и средните предприятия. За дефиницията на МСП Използват се най-вече количествените показатели, критерият за размер на служителите и икономическият критерий за годишния оборот и сумирането на икономическите резултати във финансовите отчети. Количествените критерии улесняват категоризирането на бизнеса по размери, но съдържат недостатъка на липсата на увереност и липсата на достъп до докладваните данни. Незаменима е необходимостта от включване на качествени характеристики на предприятията при сортирането им в класове. МСП се наименуват според критерии за размери, но характеристиките на управлението, структурата на собствеността и други неизмерими аспекти ги отличават от големите предприятия по-лесно, отколкото количествените показатели.

Подпомагането на МСП в усилията им за дигитализация включва посрещане на редица критични нужди. Достъпът до финансиране е един от най-критичните, тъй като МСП често се нуждаят от подкрепа, за да инвестират в инициативи за цифровизация, покривайки разходи като хардуер, софтуер и обучение на служители. Наред с това, програмите за обучение и развитие на уменията са от съществено значение за оборудването на служителите на МСП с цифровите умения, необходими за ефективното използване на технологиите. МСП често нямат вътрешния експертен опит, необходим за справяне със сложността на цифровизацията, което прави консултантските и консултантските услуги ценен ресурс. Тези услуги могат да насочват МСП при избора на технологии, разработването на стратегия и управлението на риска, като гарантират по-плавно пътуване до дигитализация, те обаче също струват немалко.

Заплахите от киберпрестъпления, глобалната корупция и бързите технологични промени са предизвикателства за компаниите, внедряващи технологиите на Индустрия 4.0. Предприятията трябва да отговарят на стандартите за съответствие, за да гарантират, че дейностите на организацията са в съответствие със съществуващите разпоредби. Стандартите за съответствие следва да се разбират както като съответствие със законовите изисквания, така и като етични стандарти. Съответствие означава изпълнение на всички

задължения на организацията. Изискванията, на които организацията трябва да отговаря, включват приложимото законодателство (закони, наредби и други нормативни актове) и има малка свобода в това отношение. Наред с това, организацията следва да отговаря на различни доброволни задължения, като индустриални или организационни стандарти, кодекси, принципи на добро управление, както и социални и етични норми, признати в организацията.

ВТОРА ГЛАВА - МЕТОДИКА ЗА ПОВИШАВАНЕ НА КИБЕРСИГУРНОСТТА В МАЛКИЯ И СРЕДЕН БИЗНЕС В БЪЛГАРИЯ

2.1 Първи етап – идентифициране и управление на рисковете за малкия и среден бизнес в България, свързани с дигитализацията

МСП са по-уязвими в сравнение с големите компании по време на периоди на икономическа и финансова рецесия, като причините са предпоставени от техните характеристики – трудност при преструктуриране или съкращаване, ниска степен на диверсификация на дейностите, по-крехка финансова структура, зависимост от външни източници на финансиране. Пандемичната криза изостря тези уязвимости, МСП реагират късно на предизвикателствата, а причините за това са най-вече в ограничените ресурси — по-конкретно недостиг на финанси и малък паричен буфер — пропуски в експертизата и уязвимости в отношенията с клиенти и доставчици.

В бизнес литературата се посочва, че рисковете за МСП при посрещането на последиците от икономическата криза се основават на липсата на финансови ресурси и високата цена на капитала, наред с недостига на административни и технически възможности.

Пандемичната криза изостря трудностите, пред които са изправени МСП и определя необходимостта от преоценка на този сектор предвид мястото и ролята, която има той в българската икономика, тъй като е дълбоко интегриран в икономическата и социална структура не само на страната, но и Европа – припомняме, че в ЕС МСП представляват 99,8% от общия брой компании, осигуряват 65% от работните места и генерират 53% от добавената стойност. От друга страна, въпреки уязвимостите, МСП са по-гъвкави и адаптивни от големите компании (характеристики, които могат да им позволят да реагират

правилно и бързо по време на криза), което се дължи на техния размер, вид на собственост и йерархични структури, близост до лицата, вземащи решения от клиенти и други заинтересовани страни, което позволява да се получи ценна пазарна информация. Наред с това, пандемията създава бизнес възможности в определени области като електронна търговия, доставки и мобилни приложения със солиден технологичен характер. В същото време обаче води до значителни промени в потребителското поведение, една от които е повишеният фокус върху онлайн пазаруването и дейностите въобще. Ето защо компаниите трябва да се адаптират към тези промени (които вероятно ще бъдат необратими), за да предложат нова стойностна оферта, базирана на иновативни технологични решения чрез инвестиции в цифровизация.

За да се справят с предизвикателствата, породени от кризата с COVID-19 и последващата рецесия и, едновременно с това, да се възползват от възможностите, възникнали през този период, МСП трябва да бъдат по-устойчиви. Устойчивостта на МСП включва креативност и иновации (като предприемачески умения) за посрещане на нуждите на клиентите и тенденциите на пазара. Въпреки това, тя самата като цяло се обуславя от устойчивостта на екосистемите на предприятието – следователно правителствената подкрепа и публичните политики са от решаващо значение за устойчивостта на МСП, за да може генерализирането на новите технологии на тяхното ниво да стимулира техния устойчив растеж, за генерализирането на новите цифрови технологии и прилагането на различни иновативни инструменти на четвъртата индустриална революция.

Ограничените финансови ресурси, както и динамичният и същевременно фрагментиран пазар ограничават диверсификацията на операциите и асортимента, предоставяни от сектора на МСП, което значително увеличава риска от бизнес провал поради фалит на тези компании[18]. Наред с това, в малките предприятия процесът на управление, за разлика от по-големите компании, често се пренебрегва и има по-тесен обхват, което също допринася за появата на множество заплахи за тяхната дейност. В същото време Jindrichovska отбеляза, че финансовото състояние на малките предприятия е

[18] Ojala, Arto, and Hannakaisa Isomäki. 2011. Entrepreneurship and small businesses in Russia: A review of empirical research. Journal of Small Business and Enterprise Development 18: 97–119

пряко и значително засегнато от техните собственици[19]. Авторката посочва, че наред с други личните аспекти са най-тясно свързани с вероятността от несъстоятелност на предприятията, което трябва да се вземе предвид в модела за оценка на риска от несъстоятелност. Тези специфични характеристики на дейността на сектора на МСП означават, че идентифицирането и измерването на техния финансов риск трябва да бъде различно от това в големите предприятия. Липсата на ресурси, позволяващи на МСП да реагират бързо на вътрешни и външни заплахи, означава, че те трябва да възприемат стратегията за управление на риска в по-голяма степен от големите организации[20].

МСП са признати за ключови двигатели на икономическия растеж и социалното развитие в световен мащаб, които допринасят за повече от 50% от данъците, 60% от БВП, 70% от технологичните иновации и 80% от цялата заетост в централните райони. Предприятията от сегмента имат присъщи характеристики, които ги отличават от по-големите компании, като по-голяма гъвкавост в отговор на промените и по-специализирани в техните способности.

Дигиталната трансформация размива границите между индустриите, носи стратегически и организационни промени и предизвиква конкурентоспособността на предприятията. Поради неадекватни вътрешни и външни ресурси, ограничен достъп до външно знание и неясни иновационни стратегии в сравнение с по-големите компании, много МСП са се сблъскали с бариери в цифровизацията от технически, технологични, организационни и правни аспекти. Междувременно непрекъснато променящата се бизнес среда след кризата с covid-19 заплашва устойчивото представяне на МСП, което ги принуждава да приемат цифрови технологии, за да се конкурират и да останат живи. Това предполага, че оцеляването на МСП ще бъде изправено пред предизвикателство без особено внимание към потенциалните рискове в една развиваща се технологична ера. Управлението на риска е един от основните подходи за МСП за справяне с несигурността и постигане на оперативен успех. В сравнение с големите предприятия, МСП с оскъдни ресурси са изправени пред повече трудности, когато става въпрос за управление на риска.

[19] Jindrichovska, Irena. 2013. Financial Management in SMEs. European Research Studies 16: 79–96

[20] Verbano, Chiara, and Karen Venturini. 2013. Managing risks in SMEs: A literature review and research agenda. Journal of Technology Management & Innovation 8: 186–97

Методите за управление на рисковете варират от по-големи компании до малки компании, в резултат на това МСП трябва да възприемат подходящи стратегии за управление на риска в съответствие със собствените си характеристики. Все още обаче липсва разбиране на съответните стратегии за управление на риска, особено в контекста на цифровата трансформация.

На първо място в контекста на пазарния риск могат да бъдат посочени множеството кризи от различен характер, породени от Covid-19 и тези по веригата на доставки. Изследванията показват, че избухването на COVID-19 има неблагоприятен ефект върху непрекъснатостта на бизнеса. МСП са предразположени да страдат при такива условия поради своята уязвимост към бързите промени на заобикалящата ги макросреда. В резултат на това е от решаващо значение да се възприемат стратегии за дигитална трансформация, за да се справят с прекъсванията в работата и веригата за доставки на пандемията. Предишно проучване показва, че кризите с covid-19 се считат за основни двигатели за МСП да пренасочат бизнеса си от офлайн физически магазини към онлайн магазини поради случаите на блокиране. Някои автори също така подчертават значението на цифровата трансформация за смекчаване на рисковете по веригата на доставки и постигане на устойчивост. Стратегии като достъп до мрежата за отворени иновации чрез цифровизация обаче могат да застрашат оцеляването на МСП. Проблеми като загуба на сила при договаряне над доставчиците, нестабилни партньорства в координацията, загуба на конкурентни предимства в конкуренцията биха възникнали в голяма степен, ако бъдат изложени на по-несигурни глобални икономически пазари.

Рискът е ключов фактор в икономическия живот, тъй като хората и компаниите правят неотменими инвестиции в научни изследвания и разработване на продукти, съоръжения и оборудване, инвентар и човешки капитал, без да знаят дали бъдещите парични потоци от тези инвестиции ще бъдат достатъчни, за да компенсират дълга и собствения капитал[21].

Напоследък киберсигурността се превръща в основен проблем на ИТ технологиите поради значението на това явление в редица области, сред които националната сигурност и световната търговска система. Киберсигурността е дефинирана като „*съвкупност от*

[21] Kimball, R. C., Failures in risk management. New England Econ. Rev. 2000, January/February 3-12

инструменти, политики, концепции за сигурност, предпазни мерки за сигурност, насоки, подходи за управление на риска, действия, обучение, най-добри практики, уверения и технологии, които могат да се използват за защита на киберсредата и организацията и активите на потребителя“[22]. Значението на киберсигурността за конкретни български институции не може да бъде пренебрегнато, тъй като всяка успешна кибератака срещу тях ще има огромен ефект върху националната сигурност на България, например като засегне нейната икономическа стабилност. Мениджърите на малък бизнес страдат от липса на знания и осъзнаване на важността на инструментите за сигурност, което влияе пряко на скоростта на приемане на киберсигурността. Следователно може да е необходимо разбирането на този актуален проблем в съответствие с гледната точка на управлението.

В наши дни управлението на риска се превръща в сериозен проблем, който обикновено засяга представянето на МСП поради различни причини като липса на ресурси и дефицит на механизми, които биха могли да подкрепят тяхната дейност по управление на риска в общ план. Наред с това, МСП, подобно на големите фирми, винаги са изправени пред различни рискове – важното е, че тяхното съществуване е по-уязвимо във всеки момент поради малкия размер на техните финансови и нефинансови ресурси. Обикновено бизнес стратегиите демонстрират по-малко внимание към последиците от управлението на риска, докато няколко стратегически хода, като избягване, контрол и сътрудничество, биха могли да намалят несигурността. Подценяването на рисковете води до злощастни последици, които обикновено засягат както материалните, така и нематериалните активи и, дори по-лошо, водят бизнеса към фалит[23].

2.2 Втори етап – законодателни инициативи в подкрепа на киберсигурността

Местни закони за защита на данните и обхват

- Конституция на Р. България (чл. 32 и чл. 34) – поставя основите на основното право на личен живот;

[22] I. T. Union, “Series X: Data Networks, Open System Communications and Security: Telecommunication security - Overview of cybersecurity,” pp. 2—-3, 2008.

[23] Hollman and S. Mohammad-Zadeh, “Risk management in small business,” J. Small Bus. Manag., vol. 1, pp. 47–55, 1984

- Общ регламент за защита на данните (GDPR) – ЗЗЛД се прилага заедно с GDPR с цел осигуряване на допълнителна защита в случаите, когато GDPR не съдържа специфична разпоредба;
- Закон за защита на личните данни – (ЗЗЛД) – основният закон за защита на личните данни в България, прилага GDPR;
- Закон за електронните съобщения – урежда обществените отношения, свързани с осъществяването на електронни съобщения; включва някои разпоредби, свързани със защитата на личните данни;
- Правилник за дейността на Комисията за защита на личните данни и нейната администрация – КЗЛД – подзаконов нормативен акт.

Органи за защита на данните

- Комисията за защита на личните данни (Комисията);
- Инспекторат към Висшия съдебен съвет (Инспекторатът)

Санкции и при неспазване на разпоредбите, уредени в гореизброените нормативни актове:

Административни санкции:

Прилага се GDPR. При други нарушения на разпоредбите на ЗЗЛД, които не са предвидени в GDPR, Комисията/Инспекторатът може да наложи санкция в размер до 5000 лв. (2500 евро). При повторно нарушение следва двойна санкция. Съгласно ЗЗЛД Комисията може да налага глоби и административни мерки, но няма правомощия за принудително изпълнение. Изпълнението на санкциите се извършва по отделно административно производство по Закона за административните нарушения и наказания.

Наказателни санкции:

Който създава, придобива за себе си или за другиго, внася или по друг начин разпространява компютърни програми, пароли, кодове или други подобни данни за достъп до информационна система или част от нея с цел извършване на определени престъпления по НК. (чл. 171 (3), чл. 319а, чл. 319б, чл. 319в или чл. 319г), грози наказание лишаване от свобода до две години. Когато се разгласят лични данни, класифицирана информация или

друга защитена от закона тайна и нарушението не съставлява по-тежко престъпление, наказанието е лишаване от свобода до три години.

Други:

Трети страни, които претърпят вреди в резултат на нарушение на съответното законодателство, могат да предявят искове за обезщетение.

Регистрация / уведомяване / оторизация

Изискването за регистрация на администраторите на лични данни отпада в съответствие с GDPR и такава регистрация вече не е необходима.

Комисията поддържа следните регистри:

- публичен регистър на администраторите и обработващите, назначили ДЛЗД;
- публичен регистър на акредитираните сертифициращи органи;
- публичен регистър на кодексите за поведение по чл. 40 от GDPR;
- вътрешен регистър за нарушения на GDPR и Закона и предприетите мерки по чл.58, §2 от GDPR;
- вътрешен регистър за уведомленията за нарушение на сигурността на личните данни по чл. 33 и чл. 67 от GDPR.

Инспекторатът поддържа и последните два вида регистри.

2.3 Трети етап – институционални реакции в случай на киберпрестъпление

В България киберсигурността и защитата на личните данни се регулират основно от следните законодателни инструменти:

- Законът за киберсигурността от 2018 г.;
- Общия регламент за защита на данните (Регламент (ЕС) 2016/679) (GDPR), пряко приложим в България;
- Законът за защита на личните данни от 2002 г. (последно изменен през 2019 г.), който беше преразгледан през 2019 г. за прилагане на GDPR.

Двете правни рамки се прилагат паралелно. Техният предмет е свързан дотолкова, доколкото законодателят е установил формални механизми за сътрудничество между надзорните органи по киберсигурността и Комисията за защита на личните данни (КЗЛД) в

случаите, когато инцидент със сигурността би представлявал и нарушение на сигурността на личните данни.

В България Законът за киберсигурността прилага Директивата за сигурността на мрежите и информационните системи (Директивата NIS, Директива (ЕС) 2016/1148) с минимални дерогации и отклонения от оригиналния текст на Директивата. Наред с това, Директивата относно мерките за високо общо ниво на киберсигурност в Съюза (Директива NIS 2, Директива (ЕС) 2022/2555) е публикувана в Официален вестник на Европейския съюз на 27 декември 2022 г. и влиза в сила от от 16 януари 2023 г. Съгласно член 41 от Директивата NIS 2 до 17 октомври 2024 г. държавите членки трябва да транспонират нормативния акт в националното си законодателство, а законите за транспониране се прилагат от 18 октомври 2024 г. На същата дата Директивата NIS ще бъде отменена.

Законът за киберсигурността съдържа съществен набор от правила, насочени към решаване на проблема с киберсигурността чрез холистичен подход. Той очертава конкретните отговорности и задължения, които юридическите лица, регулаторните органи и властите трябва да спазват, и определя механизми за предотвратяване и реагиране в случаи на кибератаки и други инциденти. Нормативният акт идентифицира основните отговорни институции и тяхната област на компетентност, въвежда категорията оператори на основни услуги и доставчици на цифрови услуги и определя техните отговорности и задължения във връзка с необходимите мерки за сигурност и процедури за уведомяване на съответните органи в случай на инциденти, свързани с киберсигурността.

Решение 192 от 09.04.2019 г. на Министерския съвет предвижда създаването на допълнителни изпълнителни органи, отговарящи за мрежовата и информационна сигурност в жизненоважни публични сектори като енергетиката, транспорта, здравеопазването, доставката на прясна питейна вода и цифровата инфраструктура. Решението очертава и методологията и специфичните критерии за определяне на основните обществени услуги, за които се прилагат специфичните нормативни изисквания.

Законът за киберсигурността определя специфичните правомощия на регулаторните органи, отговарящи за осигуряване на спазването на закона, като например Съвета за киберсигурност. Той дефинира ясни и подробни правила относно йерархичната позиция,

сътрудничеството и комуникацията с други държавни органи, като ДАНС, министъра на отбраната и министъра на вътрешните работи. Сътрудничеството и координацията между различни държавни институции са основни механизми за развитие на безопасна и устойчива цифрова среда. Вследствие на това Законът за киберсигурността предвижда създаването на Национален център за реагиране при инциденти в областта на информационната сигурност (CERT България), както и на Секторните отдели за реакция при инциденти с компютърната сигурност (Секторните CSIRT) и Национално звено за единичен контакт за общ мониторинг на проблемите на мрежовата и информационната сигурност, както и трансграничното сътрудничество с другите държави-членки на ЕС.

Законът за киберсигурността предвижда пълно и цялостно прилагане на Директивата NIS чрез приемане на подзаконови актове, като Наредба за минимални изисквания за мрежова и информационна сигурност 2019 г. Наредбата предвижда минималните специфични изисквания за мрежова и информационна сигурност, които задължените лица, доставчиците на съществени и цифрови услуги, публичните и регулаторните органи и другите доставчици на обществени услуги, трябва да спазват с цел създаване на устойчива и стабилна цифрова среда.

На ниво ЕС, Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 г. относно ENISA и относно сертифицирането на киберсигурността на информационните и комуникационните технологии и Регламент (ЕС) № 526/2013 за отмяна установява целите, задачите и организационните въпроси, свързани с ENISA и рамка за създаването на европейски схеми за сертифициране на киберсигурността за с цел осигуряване на адекватно ниво на киберсигурност за ИКТ продукти, ИКТ услуги и ИКТ процеси в ЕС, както и с цел избягване на фрагментацията на вътрешния пазар по отношение на схемите за сертифициране на киберсигурността в ЕС.

Тясно свързаният въпрос за защита на личните данни и съответните изисквания за техническите и организационни мерки, които трябва да прилагат администраторите и обработващите, както и режимът на уведомяване, приложим в случай на нарушение на сигурността на личните данни, се регулират от GDPR. На местно ниво Законът претърпява цялостна промяна през 2019 г., за да отговори на новата обща регулаторна рамка и да

приложи Директивата за защита на данните по отношение на правоприлагането (Директива (ЕС) 2016/680).

Следните конкретни правни области са извън общия обхват на приложение на Закона за киберсигурността и се регулират от специфични секторни закони и разпоредби:

- комуникационните и информационните системи за обработка на класифицирана информация по смисъла на Закона за защита на класифицираната информация (достъпен само на български език тук), който установява законови изисквания за защита на класифицирана информация от неоторизиран достъп (включително режим на уведомяване при инциденти със сигурността). и подробна рамка на мерките за сигурност). Съответният надзорен орган е Държавната комисия по сигурността на информацията.
- мрежите и информационните системи на Министерството на отбраната, Министерството на вътрешните работи, Агенцията, Държавна агенция "Разузнаване", Държавна агенция "Технически операции", Национална служба "Разузнаване" и Национална служба за защита, която не е свързана с електронните административно обслужване и електронен обмен на документи между административните органи. Съответните изисквания за мрежи и информационни системи и тяхното управление и контрол са предмет на условия и процедури, определени вътрешно в тези административни органи.
- предприятия, предоставящи обществени електронни съобщителни мрежи и/или услуги по смисъла на Закона за електронните съобщения, който установява специфични законови изисквания за защита на целостта и сигурността на електронните съобщителни мрежи и услуги, поверителността на съобщенията, както и за защита на потребителите данни, включително режим на уведомяване в случай на пробиви в сигурността или нарушения на целостта. Съответният надзорен орган е Комисията за регулиране на съобщенията (КРС). През 2021 г. Законът за електронните съобщения беше изменен с цел въвеждане на новите задължения и изисквания съгласно Директивата за създаване на Европейски кодекс за електронни съобщения (Директива (ЕС) 2018/1972).
- доставчици на удостоверителни услуги по смисъла на член 3, параграф 19 от Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги за електронни

транзакции на вътрешния пазар и Директива за отмяна 1999/93/ЕС, който също съдържа изисквания за прилагане на технически и организационни мерки във връзка с предоставяните доверителни услуги, както и режим на уведомяване в случай на пробиви в сигурността или загуба на интегритет. Съответният надзорен орган на местно ниво е КРС.

Наред с това, съгласно изискванията на Закона за платежните услуги и платежните системи, доставчиците на платежни услуги, които по принцип не попадат в обхвата на Закона за киберсигурността, трябва да прилагат специфични мерки за сигурност и да уведомяват надзорния орган в случай на значителен оперативен инцидент или инцидент със сигурността. Съответният надзорен орган е Българската народна банка.

Съветът по киберсигурност е основният надзорен орган по въпросите на киберсигурността в Република България. Членовете му включват 18 правителствени служители, включително осем министри и ръководители на основните органи за национална сигурност и правоприлагане. Съветът функционира като консултативен и координиращ орган към Министерския съвет и има за задача да анализира рисковете и киберзаплахите, да разработва методи за противодействие и да предлага конкретни решения. Прерогативите на Съвета също така включват повишаване на необходимия експертен капацитет и развитие на съществуващите човешки ресурси, наред с технологични, инфраструктурни, финансови и организационни компоненти. Съветът по киберсигурност има и задачата да създаде и предложи национална стратегия за киберсигурност и пътна карта за нейното прилагане.

Съветът действа като координационен орган между Министерския съвет, националното Единно звено за контакт и Съвета по сигурността към Министерския съвет. Освен това е натоварен с разработването на национален план за управление на киберкризи и хармонизирането на секторните политики.

Националният координатор по киберсигурност е лице, номинирано от министър-председателя, което изпълнява важна поддържаща роля на Съвета по киберсигурност. Основните му отговорности включват:

- изготвяне и предлагане на промени в Националната стратегия за киберсигурност и приложимата пътна карта;

- поемане на активна роля в развитието на Националната координационна и организационна мрежа за киберсигурност, заедно с мерките за осигуряване на нейната надеждност, сигурност и устойчивост;
- поемане на активна роля в създаването и развитието на Националния киберситуационен център и координиране на действията и цялостна реакция при заплахи от киберкризи и заплахи от хибриден характер; и
- осигуряване на поддръжка в случаи на кибератаки или хибридни атаки.

Държавната агенция „Електронно управление“ е специален административен орган, който отговаря за предоставянето на електронен достъп до административни услуги на широката общественост и контролира дейността на други административни органи в тази насока. Председателят на Държавната агенция „Електронно управление“ има голямо разнообразие от изпълнителни правомощия съгласно Закона за електронното управление, които са допълнително разширени в Закона за киберсигурността. Той отговаря за провеждането на държавната политика по отношение на мрежовата и информационна сигурност, има правомощия да издава методически указания и да координира прилагането на политиките за мрежова и информационна сигурност и може допълнително да удостоверява съответствието на информационните системи, внедрени от административните органи, с изискванията за мрежова и информационна сигурност. Председателят е длъжен да упражнява контрол върху администрациите за спазване на тези изисквания.

2.4 Четвърти етап – превенция на киберпрестъпността, засягаща малкия и среден бизнес в България

МСП разчитат изключително много на критични за бизнеса данни – информация за клиенти, оферти, поръчки и данни за плащане – и на практика не могат да работят нито ден без тях. Ето защо компаниите, независимо от размера, трябва редовно да правят резервни копия на важните си данни като първа ключова стъпка от превенцията на киберпрестъпленията и да се уверят, че тези архиви са скорошни и могат да бъдат възстановени. Правейки това, организациите гарантират, че техният бизнес може да продължи да функционира след въздействието на наводнение, пожар, физически щети или кражба. Наред с това, ако имат резервни копия на данните, които могат бързо да бъдат възстановени, не могат да бъдат изнудвани от атаки на ransomware.

Първа стъпка тук е идентифицирането на основните данни – информацията, без която бизнесът не би могъл да функционира. Обикновено това включва документи, снимки, имейли, контакти и календари, повечето от които се съхраняват само в няколко общи папки на компютъра, телефона, таблета или мрежата. Независимо дали се намират на USB памет, на отделно устройство или отделен компютър, достъпът до архивите на данни трябва да бъде ограничен, така че те:

- да не са достъпни за персонала
- да не са постоянно свързани (физически или през локална мрежа) с устройството, което съдържа оригиналното копие.

Ransomware (и всеки друг злонамерен софтуер) често може автоматично да се премести в прикачено хранилище, което означава, че всяко подобно архивиране също може да бъде заразено, оставяйки компанията без резервно копие, което да се възстанови. За по-голяма устойчивост резервните копия трябва да се съхраняват на друго физическо и/или виртуално място, така че кражба да не доведе до загуба на двете копия – решенията за съхранение в облак са рентабилен и ефикасен начин за постигане на това.

Редица МСП използват облачно хранилище по време на ежедневната си работа, без дори да си дават сметка за това – освен ако не работят със собствен имейл сървър, имейлите вече се съхраняват „в облака“. Използването на облачно хранилище, където доставчик на услуги съхранява данните в своята инфраструктура означава, че информацията е физически отделена от физическото местоположение. Този тип услуги предлагат и високо ниво на наличност. Доставчиците могат да предоставят на организацията съхранение на данни и уеб услуги, без да е необходимо тя да инвестира предварително в скъп хардуер. Повечето доставчици предлагат ограничено пространство за съхранение безплатно и по-голям капацитет за съхранение за минимални разходи за малкия бизнес.

Не всички доставчици на услуги са еднакви, но пазарът е сравнително зрял и повечето вече са възприели редица добри практики за сигурност. Предавайки значителни части от ИТ услугите на доставчик, МСП се възползват от специализирана експертиза, която по-малките организации вероятно биха се затруднили да оправдаят по отношение на разходите.

Факт е, че при МСП архивирането много често е изместено от редица други по-важни задачи, но повечето мрежови или облачни решения за съхранение вече позволяват да се правят резервни копия автоматично – например, когато нови файлове от определен тип се записват в определени папки. Използването на автоматизирани архиви не само спестява време, но също така гарантира, че е налице най-новата версия на файловете, ако бизнесът има нужда от тях.

Много готови решения за архивиране са лесни за настройка и достъпни като се има предвид критичната за бизнеса защита, която предлагат. Когато мениджмънтът избира решение, трябва също така да вземе предвид колко данни трябва да бъдат архивирани и колко бързо трябва да има достъп до данните след всеки инцидент[24].

Зловреден софтуер (известен също като „малуеър“) е софтуер или уеб съдържание, което може да навреди на организацията. Най-известната форма на зловреден софтуер са вирусите – самокопиращи се програми, които заразяват легитимен софтуер.

Антивирусният софтуер, който често се включва безплатно в популярните операционни системи, трябва да се използва на всички компютри и лаптопи.. Смартфоните и таблетите може да изискват различен подход.

Изтеглянето на приложения за мобилни телефони и таблети трябва да се случва само от одобрени от производителя магазини (като Google Play или Apple App Store). Тези приложения се проверяват, за да осигурят определено ниво на защита от зловреден софтуер. Служителите на компанията не бива да имат права да изтеглят приложения на трети страни от неизвестни доставчици/източници, тъй като те няма да бъдат проверени. Акаунтите на персонала трябва да имат достатъчно достъп, необходим за изпълнение на тяхната роля, с допълнителни разрешения (т.е. за администратори), давани само на тези, които се нуждаят от тях. Когато се създават административни акаунти, те следва да се използват само за тази конкретна задача, като стандартните потребителски акаунти се използват за обща работа.

[24] Dojkovski, S.; Lichtenstein, Sharman; and Warren, Matthew J., (2006) "Challenges in Fostering Information Security Culture in Small and Medium Size Enterprises", in preceding of 5 th European Conference on Information Warfare and Security, 1-2 June, 2006. National Defense College, Helsinki, Finland

За цялото ИТ оборудване (таблети, смартфони, лаптопи и персонални компютри) мениджмънтът трябва да се увери, че софтуерът и фърмуерът винаги са актуализирани с най-новите версии от разработчици на софтуер, доставчици на хардуер и продавачи. Прилагането на тези актуализации е едно от най-важните неща, които МСП могат да направят, за да подобрят сигурността. Операционните системи, програмите, телефоните и приложенията трябва да бъдат настроени на „автоматично актуализиране“, когато това е опция. В даден момент тези актуализации вече няма да са налични (тъй като продуктът достигне края на поддържания си живот) – тогава трябва да се обмисли замяната му с модерна алтернатива[25].

Изключително изкушаващо е да се използват USB устройства или карти с памет за прехвърляне на файлове между организации и хора – достатъчно е обаче само един потребител да включи по невнимание заразен стик (например, USB устройство, съдържащо злонамерен софтуер), за да опустоши цялата организация. Когато устройствата и картите се споделят открито, става трудно да се проследи какво съдържат, къде са били и кой ги е използвал. Може да се намали вероятността от заразяване чрез:

- блокиране на достъпа до физически портове за повечето потребители;
- използване на антивирусни инструменти;
- позволение само одобрени устройства и карти да се използват във вашата организация - и никъде другаде

Тези директиви следва да станат неразделна част от фирмената политика, за да се предотврати излагането на организацията на ненужни рискове. Мениджмънтът може също така да стимулира служителите да прехвърлят файлове чрез алтернативни средства като имейл или облачно хранилище, вместо чрез USB[26].

Мобилните технологии вече са съществена част от съвременния бизнес, като все повече данни се съхраняват на таблети и смартфони – нещо повече, тези устройства сега са

[25] Doherty, N.F. & Fulford, H. (2006) Aligning the Information Security Policy with the Strategic Information Systems Plan, Computers & Security, 25(2), 55-63

[26] Johnson, D.W. & Koch, H. (2006) Computer Security Risks in the Internet Era: Are Small Business Owners Aware and Proactive? In Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06), IEEE Society Press.

толкова мощни, колкото традиционните компютри и, тъй като често напускат безопасността на офиса, те се нуждаят от още по-голяма защита от десктоп оборудването.

Подходящо сложен ПИН код или парола, за разлика от простите, които могат лесно да бъдат отгатнати или извлечени от профилите в социалните медии, ще попречат на обикновения престъпник да получи достъп до служебния телефон. Много устройства вече включват разпознаване на пръстови отпечатъци за заключване, без да е необходима парола. Въпреки това, тези функции не винаги са активирани.

На персонала е по-вероятно да бъдат откраднати (или да ги загубят) таблети или телефони, когато са далеч от офиса или дома. За щастие, по-голямата част от устройствата включват безплатни уеб базирани инструменти, които са безценни, когато то изчезне. Те могат да бъдат използвани за:

- проследяване на местоположението на устройството;
- отдалечено заключване на достъпа до устройството (за да се попречи на някой друг да го използва);
- дистанционно изтриване на данните, съхранени на устройството;
- извличане на резервно копие на данните, съхранени на устройството.

Настройването на тези инструменти на всички устройства на организацията може да изглежда обезсърчително в началото, но с помощта на софтуер за управление на мобилни устройства настройването към стандартна конфигурация може да се случи с едно щракване.

Без значение какви телефони или таблети използва компанията, важно е те да се поддържат актуални по всяко време. Всички производители (Windows, Android, iOS) пускат редовни актуализации, които съдържат критични актуализации за защита. Този процес е бърз, лесен и безплатен, а устройствата трябва да бъдат настроени да се актуализират автоматично, когато е възможно. Мениджмънтът на МСП трябва да се увери, че персоналът знае колко важни са тези актуализации и да обясни как да ги направят служителите, ако е необходимо. Подобно на настолните компютри, в даден момент тези актуализации вече няма да са налични, тъй като устройството ще достигне края на своя поддържан живот, в който момент трябва да се обмисли замяната му с модерна алтернатива.

Точно както операционните системи на устройствата на организацията, всички приложения също трябва да се актуализират редовно с корекции от разработчиците на софтуер. Тези актуализации не само ще добавят нови функции, но и ще "закърпят" всички открити дупки в сигурността. И по този параграф мениджмънтът трябва да се увери, че служителите знаят кога актуализациите са готови, как да ги инсталират и че е важно да го направят веднага.

Когато се използват обществени Wi-Fi точки (в хотели или кафенета), няма начин лесно да се разбере кой ги контролира или да се докаже, че тя принадлежи на когото мислите, че е. Ако служебно устройство се свърже с тези точки, някой друг може да получи достъп до:

- това, върху което служителят работи, докато е свързан;
- лични данни за вход, които много приложения и уеб услуги поддържат.

Най-простата предпазна мярка е служебните устройства не се свързват с интернет чрез неизвестни точки, а вместо това да се използва мобилна 3G или 4G мрежа, която има вградена защита. Това означава, че може също да се използва „тетъринг" (където другите устройства като лаптопи споделят същата 3G/4G връзка) или безжичен „донгъл", предоставен от мобилната мрежа. Може също така да бъдат използвани виртуални частни мрежи (VPN) – техника, която криптира данните, преди да бъдат изпратени по интернет. Ако се използва VPN на трети страни, ще трябва техническата възможност за конфигурация. Важно е да се разчита само на VPN, предоставени от реномирани доставчици на услуги[27].

Служебните лаптопи, компютри, таблети и смартфони ще съдържат много от критичните за бизнеса данни – личната информация на клиентите, както и подробности за онлайн акаунтите, до които има достъп компанията. От съществено значение е тези данни да са достъпни за мениджмънта, не и за неоторизирани потребители. Паролите – когато са

[27] Dimopoulos, V., Furnell, S.M., Jennex, M. & Kritharas, I. (2004) Approaches to IT Security in Small and Medium Enterprises, in Proceedings of the 2nd Australian Information Security Management Conference 2004, Perth, Australia

използвани правилно – са безплатен, лесен и ефективен начин за предотвратяване на достъпа на неоторизирани потребители до вашите устройства.

Може да се парола за заключване на екрана, ПИН или друг метод за удостоверяване (като пръстов отпечатък или отключване с лице). Ако се използва предимно пръстов отпечатък или отключване с лице, ще се въвежда парола по-рядко, така че ръководителите могат да помислят за настройка на дълга парола, която е трудна за отгатване.

Защитата с парола не е само за смартфони и таблети. Мениджмънтът на МСП следва да се увери, че за цялото офис оборудване (лаптопи и персонални компютри) използва се продукт за криптиране (като BitLocker за Windows) с помощта на Trusted Platform Module (TPM) с PIN или FileVault (на macOS), за да се стартират устройствата. Повечето съвременни устройства имат вградено криптиране, но все пак може да се наложи криптирането да бъде включено и конфигурирано.

Ако е налична дадена опцията да двуфакторна идентификация (известно още като 2SV) за който и да е от организационните акаунти, тя трябва да бъде използвана – това добавя голямо количество сигурност на цената на не много допълнителни усилия. 2SV изисква два различни метода за „доказване“ на самоличност, преди да може да се използва услуга, обикновено парола плюс един друг метод. Това може да е код, е изпратен на определен смартфон (или код, който е генериран от четец на карти на банка), който трябва да бъде въведен в допълнение към паролата.

Отговорният за ИТ политиките в организацията специалист следва да се увери, че служителите получават полезна, лесна за разбиране информация относно задаването на пароли. Те трябва да са лесни за запомняне, но трудни за отгатване от някой друг. Персоналът също така трябва да избягва използването на най-често срещаните пароли, които престъпниците могат лесно да познаят. ИТ системите сами по себе си не трябва да изискват от служителите да споделят акаунти или пароли, за да си свършат работата – всеки потребител има личен достъп до конкретни системи, а даденото ниво на достъп винаги е най-ниското, необходимо за извършване на работата, което върви ръка за ръка с минимизиране ненужното излагане на системи, до които не се нуждаят от достъп.

Специалистът, който отговаря за това как се използват паролите в организацията, може да направи редица неща, които ще подобрят сигурността. Най-важното е, че персоналът ще има десетки несвързани с работата пароли, които също трябва да запомни, така че налагането на достъп с парола до услуга в службата трябва да се налага, само ако наистина имате нужда. Когато се използват пароли за достъп до услуга, добре е да не се налагат редовни промени – те наистина трябва да се променят само когато е налице подозрение, че идентификационните данни за вход са компрометирани.

Необходимо е също така да бъде осигурено хранилище, така че служителите да могат да записват пароли за важни акаунти (като имейл и банкови) и да ги пазят (но не със самото устройство). Служителите могат да забравят паролите, което означава, че е необходимо да се помисли за инструменти, чрез които те лесно могат да ги нулират сами. МСП могат да обмислят използването на мениджъри на пароли – това са инструменти, които могат да създават и съхраняват пароли, до които се получава достъп чрез „главна“ парола. Тъй като главната парола защитава всички други, необходимо е тя да е силна, например три произволни думи.

Една от най-честите грешки е непромяната на паролите по подразбиране на производителите, с които се издават смартфони, лаптопи и други видове оборудване. Промяната трябва да се случи преди устройствата да бъдат раздадени на персонала. Въпреки това, необходимо е редовно да се проверяват устройствата и софтуера, специално за откриване на непроменени пароли по подразбиране[28].

[28] Paul Ruggiero, J.F. 2011. Cyber Threats to Mobile Phones. https://www.uscert.gov/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf последно посетен на 20.02.2024

ТРЕТА ГЛАВА - АПРОБАЦИЯ НА МЕТОДИКАТА ЧРЕЗ ЕМПИРИЧНО ИЗСЛЕДВАНЕ. АНАЛИЗ, ПРЕВЕНЦИЯ И ВЪЗМОЖНИ НАСОКИ ЗА КИБЕРСИГУРНОСТТА, ЗАСЯГАЩА МАЛКИЯ И СРЕДЕН БИЗНЕС В БЪЛГАРИЯ

3.1 Обосновка на изследването

3.1.1 Необходимост от провеждането на емпиричното изследване

В предишните две глави бяха разгледани подробно редица характеристики на киберсигурността и предпоставки за влошаването ѝ в контекста на МСП в България. Излизането от националния контекст, което личи от всеки отделен раздел, е неизбежно, тъй като, от една страна, България е пълноправна държава-членка на ЕС, а от друга, киберпрестъпността, предвид виртуалния характер на явлението, категорично надхвърля географските граници на държави и наднационални обединения. Наред с това, фактът, че България има много широка и леснодостъпна интернет инфраструктура, но изостава в институционален, законодателен и всякакъв друг практически план в мерките за борба с киберпрестъпленията, прави страната привлекателна мишена за кибератаки. Геополитическото положение, което се влошава заради конфликтите на интереси между Изтока и Запада, характерни за България поради географското ѝ положение и политическото и идеологическото минало също са предпоставка за влошаване на киберсигурността, както и за засягането на МСП от последиците от това.

Малкият бизнес има по-малко ресурси, но повече гъвкавост по отношение на вземането на решения – ето защо има голяма вероятност предложената по-горе методика, поне в частта ѝ, която се отнася до моделиране на потребителското поведение на служители и клиенти на МСП да е напълно приложима в условията у нас. За да стане ясно дали това е така, ще бъде проведено емпирично изследване, което да проучи нагласите на собствениците на малък и среден бизнес и техните клиенти по въпросите с киберсигурността. Това е необходимо, за да може, въз основа на резултатите, да се дадат препоръки за това как и в каква част да се приложи изследваната по-горе методика.

3.1.2 Обект и предмет на изследване

Обект на изследване са измеренията на киберсигурността и киберпрестъпността в контекста на малкия и среден бизнес в България, а предмет – конкретните нагласи по темата с повишаването на киберсигурността на МСП на собствениците на такъв тип бизнеси и техните клиенти.

3.1.3 Цели и задачи

Целта на емпиричното изследване е да се проведи доколко методиката, изложена във втора глава от настоящия дисертационен труд е подходяща за прилагане в условията в България. В този контекст могат да бъдат формулирани следните задачи:

- избор на метод за изследване;
- конструиране на инструментариум и подбор на извадка;
- провеждане на емпиричното изследване;
- обобщаване, представяне и коментар на резултатите;
- формулиране на апробация на методиката и препоръки за подобряване киберсигурността на МСП в България.

3.1.4 Метод на изследване

Избраният метод за изследване е анкета – една и съща карта за собствениците на бизнеси и за потребителите, което ще направи сравняването на резултатите по-лесно и удобно. Обикновено, хората не обичат да отделят време за попълване на проучвания – ето защо анкетната карта съдържа 15 затворени въпроса, първите 5 от които събират демографски данни. Участието в проучването е доброволно и анонимно, което е описано и в самото начало на картата (Приложение 1).

Извадките, с които ще се работи за целите на дисертационния труд, са твърде малки, за да може изследването да претендира за представителност. Въпросите обаче ще бъдат формулирани така, че проучването да бъде достоверно. При изготвянето на анкетната карта ще се стремим да бъдат отразени всички възможни опции за отговор, а там, където не е сигурно, че това е възможно да бъде спазено, ще бъде включена възможност "друго (моля, посочете в свободен текст). За да избегнем отказ от попълване на анкетата заради определен

въпрос, никой от тях няма да бъде задължителен – респондентите ще имат възможност свободно да пропускат въпроси и да могат успешно да завършат анкетата.

Проучването ще се разпространява чрез социалната мрежа, а при достигане на необходимия брой отговори, анкетата ще бъде затворена и скрита.

3.1.5 Групи, които ще бъдат включени, и техните характеристики

Еднакво важно за повишаване на киберсигурността на МСП е поведението на четири ключови агенти – самите предприятия (чрез техните мениджъри и служители), потребителите на продуктите и услугите им, институциите и банките (тъй като в момента, на практика, МСП не могат да съществуват без да използват услугите им). На поведението на вторите две не може да се повлияе лесно, но, за сметка на това, потребителите и представителите на бизнеса са достатъчно гъвкави, че реални промени в техните нагласи и действия могат бързо да доведат до подобряване ситуацията с киберпрестъпността в сегмента у нас. Ето защо е важно те да бъдат изследвани.

3.1.5.1 Потребители на продукти на малкия и среден бизнес

Практически всеки човек купува стоки и услуги от малък и среден бизнес, съзнателно или не. Онлайн пазаруването е вече част от ежедневието, което води до въпроса осъзнават ли потребителите какви отговорности имат по отношение собствената си и тази на търговците, от които купуват, киберсигурност. Именно това следва да се провери чрез емпиричното изследване – за целите на удобството при обработката на резултатите, необходими са 50 попълнени анкети, а след достигането на този брой отговори проучването ще бъде затворено.

3.1.5.2 Собственици и ръководители на малки и средни предприятия

Собствениците и ръководителите на МСП често имат твърде много професионални и социални роли в един и същи момент и нелеката задача да се справят с тях в условията на липса на достатъчно ресурси от различни видове. Във все по-дигитализирания свят, това отваря място за сериозни пропуски в областта на киберсигурността, които престъпниците и потенциалните такива във сигурност забелязват – ето защо и в последните години именно

МСП стават все по-чести мишени на такива атаки. Има ли осъзнаване за това и какви мерки биха предприели собствениците на бизнеси ще стане ясно от анкетирането на 50 такива.

3.2 Коментар и анализ на резултатите

3.2.1 Прилики между нагласите на потребителите и собствениците и ръководителите на малък и среден бизнес

Както вече бе уточнено по-горе, собствениците на малък бизнес са непременно и потребители на продуктите и услугите на други такива. Наред с това, тъй като за МСП е характерна по-свободна, хоризонтална вместо подчертано вертикална комуникация нагоре и надолу по ясно изразени йерархически нива, малките бизнеси остават близо до клиентите си и се смесват с тях ежедневно. Ето защо не е изненада, че отговорите на двете групи си приличат толкова много.

Липсва съвсем ясна преценка за това какъв дял в частния сектор имат МСП – това е видно както при потребителите, така и при собствениците на предприятия. До голяма степен неосъзнаването на ключовата роля на сегмента в икономиката, не само в България, а и в европейски и глобален мащаб, може да се окаже проблем от гледна точка на това, че подценявайки собственото си значение, малките бизнеси подценяват и заплахите, които възникват за сигурността им.

И при двете групи има ясно разбиране, че киберсигурността се отнася до всички – както до индивидите, така и до предприятията, без значение от техния размер. По-категорично е това мнение сред собствениците на МСП – всички те са посочили този отговор. При потребителите все още се срещат и други опции, например тази, че киберсигурността се отнася само до големите предприятия. Фактът, че МСП остават близо до клиентите си, може да подпомогне промяната на тази нагласа, ако се използват подходящи комуникационни техники.

Онлайн присъствието е задължително за малкия и среден бизнес – така мислят и потребителите, и собствениците на предприятия от сегмента. Наблюдава се силно предпочитание към положителните опции за отговор, които се отнасят до това как Мрежата

подпомага представянето на бизнесите и ги доближава до потребителите им. И при двете групи респонденти рязко спада броят отговори при отрицателните опции, които се отнасят до това, че онлайн присъствието крие и своите опасности, както за клиентите, така и за притежателите. Все пак, осъзнаването на това при собствениците на МСП е по-добро – това означава, че предприятията са готови, поне психологически в лицето на лидерите си, да се опитат за защитят потребителите си. Дали обаче ресурсите и ежедневните задължения им го позволяват е въпрос, на който отговорът е по-скоро отрицателен.

На въпроса как предпочитат да пазаруват, и двете групи разпределят отговорите си почти по равно между "*онлайн"* и "*и по двата начина"*, като предпочитанията конкретно към физическите обекти са малко и, и при потребителите, и при собствениците на МСП, идват от по-възрастните респонденти. Ето защо е положително за възможностите за подобряване на киберсигурността, че приликите при отговорите на следващите въпроси са повече от разликите.

И потребителите, и собствениците на МСП се възползват активно от възможностите да изберат по няколко опции за отговор на въпросите, които се отнасят до това от какво трябва да се притесняват потребителите и какво трябва да направят бизнесите, за да минимизират киберрисковете.

Повече потребители и повече собственици на бизнеси се притесняват от изтичането на банкова информация, отколкото от това на лични данни. Собствениците на бизнеси много ясно осъзнават необходимостта потребителите да са изключително внимателни, когато служител на МСП им поиска чувствителна информация. При потребителите осъзнаване също има, но е в много по-малка степен, отколкото при лидерите.

Всички изброени опции за отговор на въпроса Какво трябва да направят МСП, за да защитят потребителите си?, представляват мерки, коментирани по-горе в методическата втора глава на дисертационния труд. Потребителите разбират добре, че всички те в една или друга степен са важни. Собствениците на бизнеси обаче почти единодушно се съгласяват, че всички предложени мерки трябва да бъдат взети, за да се гарантира киберсигурността на потребителите и на самия бизнес – тук се включват както задълбочена проверка на служителите и минимално ниво на достъп на информация, така и чисто

технологични мерки и решения като поддържане на актуални устройства, системи и софтуери и използване на облачни услуги, сигурни интернет точки за достъп и резервни копия на данните. Притеснителен е фактът, че и потребителите, и собствениците на бизнеси не осъзнават докрай колко е важно използването на сигурни точки за достъп до Интернет – това е най-малко посочваната опция и при двете групи анкетирани.

За ролята на потребителите в гарантирането на киберсигурността и клиентите, и собствениците на МСП, считат, че е много важно те да са внимателни при това каква информация дават за себе си онлайн, да ползват, по възможност, виртуални карти, да внимават какви сайтове посещават, особено що се отнася до съмнителни линкове.

Прави впечатление тук, че най-малко хора и от двете групи избират плащането с виртуални карти – повече се набляга на даването на минимум информация в Мрежата и вниманието към сайтовете и последваните връзки.

Нагласите към работата на институциите също си приличат много и при двете изследвани групи – значителна част от респондентите считат, че властите не работят по посока подобряване киберсигурността на МСП у нас. Мнението за банковите институции е много подобно – малко потребители считат, че те могат да гарантират сигурността на данните им, както и на тези на предприятията, при собствениците на бизнеси това са малко повече представители, но общата картина остава същата.

На практика, това се дължи по-скоро на разпространеното у нас вярване, че институциите не работят, както и на факта, че от няколко години насам на практика ползването на банкови услуги е абсолютно задължително както за обикновените хора, така и за собствениците на бизнеси. Т.е. едните така или иначе не работят, по всички параграфи, така че подпомагането киберсигурността на МСП не е изключение, а другите е наложително да бъдат използвани, ето защо тревогите за това какво могат и какво не могат да гарантират биха причинили твърде много излишен, но за сметка на това ежедневен стрес. Обективно погледнато, скорошни инциденти има и на двата фронта – и от НАП, и от банка ДСК изтекоха лични и други данни на хиляди българи.

3.2.2 Разлики между нагласите на потребителите и собствениците и ръководителите на малък и среден бизнес

Разликите в нагласите на двете групи са много малки, но, за сметка на това, правят сериозно впечатление и показват, че, колкото и близо да са потребителите и собствениците на бизнеси, все пак развиването на самостоятелна дейност води до промяна в мисленето.

Най-фрапантният пример са отговорите на въпрос 12, който се отнася до това трябва ли да бъдат санкционирани служителите на МСП, ако заради техни действия компанията пострада при киберинцидент. В първата група все пак са попаднали 4 самонаети лица – те дават отговор "*не*", а мнозинството потребители считат, че наказанието за работещите е необходимо. Това подсказва, че няма да стоят така нещата при представителите на бизнеса – и наистина, болшинството тук не мислят, че трябва да санкционират служителите си. Тук обяснението е следното: с право потребителите разчитат, че работещите в бизнесите, от които те пазаруват продукти и услуги трябва да са изключително внимателни и отговорни, когато става дума за чувствителната информация, с която работят, още повече, че дигиталната следа се увеличава с всеки изминал ден. Те обаче не осъзнават добре пред какви предизвикателства, наред с все по-професионалните киберпрестъпници, са изправени МСП. Предприятията от сегмента трудно намират служители, тъй като нерядко не успяват да се конкурират с големите компании нито по отношение на строго разпределение на задачите, нито що се отнася до заплащането.

Ето защо, в повечето случаи, в малкия бизнес работят или самите му собственици, или, заедно с тях, изключително близки и доверени хора. Ето защо, обикновено, киберинцидентите са резултат от грешка на служителите, а не от злонамереност. Ако все пак се окаже второто, повечето собственици на МСП не се колебаят да направят рещителната стъпка и да се разделят с нелоялния кадър. Допускането на неволни грешки обаче не се поправя със санкции – нещо повече, липсата на наказания не означава липса на воля за справяне с проблема. Означава използване на други инструменти, които ще гарантират както лоялността на служителя в дългосрочен план, така и киберсигурността на бизнеса и неговите потребители. Тук откритото говорене за пропуска и причината да се стигне до него, за щетите, които са били причинени, поемането на отговорност от бизнеса като цяло, не само от един работник говори за зрялост на организацията.

Другата съществена разлика, която задължително трябва да бъде посочена, е в отговорите на въпроса От какво да се притесняват потребителите на МСП по отношение на тяхната киберсигурност?. Немалка част от първата група анкетирани – а именно клиентите – твърди, че място за притеснение няма. От бизнеса обаче не посочват тази опция нито веднъж. Причината е, че собствениците на МСП добре разбират киберрсиковете в голямата си част и, с наличните ресурси, се стремят да ги управляват оптимално. Това обаче става практически невъзможно при безотговорно потребителско поведение – ако клиентите не осъзнават, че киберсигурността – тяхната и на бизнесите, от които пазаруват – е отговорност в еднаква степен и за двете страни, за представителите на бизнеса ще бъде много по-трудно да защитят и двете страни.

3.3 Възможни пътища за подобряване на киберсигурността на малкия и среден бизнес в България

Емпиричното изследване показва, че изложената във втора глава на дисертационния труд методика е напълно приложима в България, що се отнася до частта й с действията, които следва да бъдат предприети от страна на МСП и на потребителите на техните продукти и услуги. Всъщност, лидерите и собствениците на предприятия от сегмента са често и съзнателни потребители на продукти и услуги от същия, най-вече защото знаят колко трудности среща едно малко предприятие с ограничените си ресурси и това да подкрепят подобни бизнеси им носи емоционално удовлетворение. Това означава, че тези хора мислят едновременно като бизнес ръководители и клиенти, а от тук следва и по-внимателното и отговорно отношение както към собствената им сигурност, така и към тази на колегите, от които пазаруват.

Наред с това, гъвкавостта, с която разполагат МСП, позволява много по-лесно да се вземат решения коя част от процесите и нужните по-нататъшни действия в областта на киберсигурността да остане в рамките на компанията и коя да бъде прехвърлена на външни контрагенти. По-малките предприятия имат облекчени процедури за финансиране на редица дейности, ето защо от вземането на решение, че е необходим бюджет за обучение на персонала до реализирането на такова няма нужда да минават месеци и години в прехвърляне на предложението нагоре и обратно надолу по множество йерархически нива.

В малките бизнеси личната комуникация е значително по-силна – това прави по-лесно ангажирането на всички служители с проблемите на киберсигурността и по-свободно докладването и обсъждането на подозрителни съобщения, без страх от наказания, както е в големите компании. По-лесно е и разкриването на злонамереност и вътрешни заплахи. Затрудненията тук обаче могат да дойдат от това, че поради недостиг на средства, особено в началото на всеки бизнес, служителите използват за работа и личен живот едни и същи устройства. Решението е специалист да прецени как може да защити добре работната част от информацията.

Потребителите, от своя страна, са добре информирани и все по-често осъзнават как е възможно данните им, особено банковата информация с увеличаването на картовите и онлайн плащанията, да изтече и какви могат а бъдат последствията от това. Много хора от първа ръка знаят, че не могат да разчитат на банките да върнат бързо загубените суми, ето защо предпочитат да бъдат по-предпазливи и сами да вземат мерки за защита, например, да използват само виртуални карти за онлайн плащания и да проверят търговеца предварително. Това значително подпомага усилията на лидерите на МСП, но, разбира се, не отменя необходимостта от полагането им. Нещо повече – при все по-голямото предлагане на стоки и услуги, по-вероятно е клиентите да изберат да купят от тези търговци (онлайн и физически), които демонстрират загриженост за киберсигурността на предприятието си и, по този начин, и за тази на потребителите.

В България, за съжаление, и властите в лицето на институциите, и банките, по-скоро затрудняват борбата с киберпрестъпността. Факт е, че ГДБОП се грижи за лесен път за докладване на инциденти в специализиран за това онлайн портал. Липсват обаче мащабни информационни кампании, насочени конкретно към МСП и потребителите на техните продукти и услуги. Разследванията на банките при докладвана фишинг атака са бавни и несигурни, а възстановяването на откраднатите суми става едва след няколко месеца, в които клиентите често са третирани като измамници, а не като потърпевши. Това означава, че методиката от втора глава е неприложима у нас в частта й за включеността на институциите и банките – факт е, че банките се опитват да предприемат действия, но те са по-скоро част от техните PR стратегии, а не последователни и целенасочени кампании.

Държавните институции пък не показват ангажираност към проблемите конкретно на МСП, въпреки че именно те представляват повече от 85% от българския частен сектор. Липсва служебна комуникация на високо ниво между банките и институциите – така става необходимо МСП да отделят ресурси не само за възстановяване на предприятието след киберинцидент, а и за докладване на едно и също нещо в различни институции и пряко участие в различни разследвания, което води до отказ от съобщаване за редица кибератаки, а от тук – до невъзможност за идентифициране реалните мащаби на киберпрестъпността срещу малкия бизнес в България и, съответно, вземане на адекватни мерки от страна на властите за ограничаването ѝ. Наред с това, законодателството категорично изостава от изобретателността на киберпрестъпниците – така, в обобщение, следващите мерки и препоръки ще бъдат съобразени с желанието и волята на МСП и техните потребители да търсят проактивно решение на проблемите с киберсигурността.

IV. ЗАКЛЮЧЕНИЕ

В днешния цифров пейзаж МСП са изправени пред нарастващи предизвикателства по отношение на киберсигурността. Въпреки размера си, те са ценни мишени за киберпрестъпниците поради ограничените си ресурси и потенциално по-слаби мерки за сигурност. МСП, подобно на по-големите организации, боравят с чувствителни данни и са изправени пред значителни финансови и репутационни рискове в случай на нарушение на сигурността на данните. За тях е от решаващо значение да признаят значението на киберсигурността и проактивно да инвестират в защитата на своите цифрови активи.

Съществува често срещано погрешно схващане, че МСП не са доходоносни цели за кибератаки. Киберпрестъпниците обаче гледат на представителите на сегмента като на лесни мишени поради техните потенциално ограничени мерки за сигурност и ресурси. От съществено значение е МСП да разберат, че не са имунизирани срещу киберзаплахи и трябва да предприемат подходящи мерки за защита на своята цифрова инфраструктура.

Малките бизнеси все по-често се сблъскват с целенасочени атаки, насочени към кражба на ценни данни, прекъсване на операциите или изнудване за плащане на откуп. По-специално, атаките на рансъмуер, при които нападателите криптират критични данни и изискват плащане, за да възстановят достъпа, стават в последните години преобладаващи.

МСП трябва да са наясно с тези заплахи и да прилагат превантивни мерки за смекчаване на рисковете. Те обаче често имат ограничени бюджети, разпределени за мерки за киберсигурност, което прави предизвикателство да се инвестира в стабилни решения за сигурност и специализиран персонал. Това ограничение ги прави привлекателни мишени за киберпрестъпниците. Намирането на рентабилни решения става от решаващо значение за МСП за укрепване на защитата им.

Предприятията от сегмента може да нямат вътрешен опит в областта на киберсигурността, което затруднява разработването и прилагането на ефективни стратегии за сигурност. Без подходящия експертен опит идентифицирането на уязвимостите и прилагането на подходящи контроли за сигурност се превръща в предизвикателство. МСП трябва да проучат възможности като аутсорсинг или ангажиране с управлявани доставчици на услуги за сигурност (MSSP), за да преодолеят тази празнина.

Служителите имат критична роля в поддържането на силни практики за киберсигурност. Много малки и средни предприятия обаче нямат адекватни програми за обучение на персонала си за информираност относно сигурността. Без подходящо обучение служителите могат да станат жертва на фишинг атаки или несъзнателно да участват в рисково онлайн поведение. МСП трябва да дадат приоритет на осведомеността относно сигурността и да обучат служителите си относно най-добрите практики.

МСП често разчитат на доставчици и трети страни за различни услуги. Тези трети страни обаче могат да въведат потенциални уязвимости в екосистемата, ето защо за МСП е от решаващо значение да оценят състоянието на киберсигурността на своите доставчици, да създадат сигурни комуникационни канали и да прилагат договорни споразумения за смекчаване на рисковете от трети страни.

Кибер заплахите непрекъснато се развиват и редовно се появяват нови техники за атака и уязвимости. МСП може да се затрудняват да бъдат в крак с най-новите тенденции и, съответно, да адаптират своите мерки за сигурност. Да бъдат информирани и проактивни при наблюдението на възникващи заплахи е от съществено значение за МСП, за да поддържат ефективна защита на киберсигурността. Те трябва да разработят цялостна стратегия за киберсигурност, която е в съответствие с техните бизнес цели и склонност към

риск, която да очертае контролите за сигурност, процедурите за реакция при инциденти и механизмите за възстановяване в случай на кибер инцидент. Наличието на план за реагиране при инцидент помага да се сведе до минимум въздействието на пробив и гарантира бърза реакция.

МСП трябва да дадат приоритет на обучението за осведоменост относно киберсигурността за всички служители. То следва да обхваща теми като разпознаване на фишинг имейли, създаване на силни пароли и безопасно използване на фирмените ресурси. Редовните обучения и кампании за осведомяване могат значително да намалят риска от човешка грешка и да подобрят цялостната позиция на сигурността на организацията. Наред с това, необходимо е да бъде наложен стабилен контрол на достъпа, за да се ограничи неоторизиран такъв до чувствителни системи и данни. Това включва прилагане на силни пароли, многофакторно удостоверяване и принципи за най-малко привилегии. Чрез ограничаване на достъпа само до онези, които го изискват, МСП могат да намалят потенциалната повърхност за атака и да минимизират въздействието от пробив.

МСП трябва да поддържат актуализирани своя софтуер и системи и незабавно да прилагат корекции за сигурност и актуализации. Софтуерът без тях може да съдържа известни уязвимости, които киберпрестъпниците могат да използват. Внедряването на процес за управление на корекциите помага за защита срещу известни уязвимости и укрепва позицията на сигурност. Защитните стени и антивирусните решения осигуряват основен слой на защита срещу различни кибер заплахи. МСП трябва да разположат стабилни такива за мониторинг и филтриране на входящия и изходящия мрежов трафик. Наред с това, на всички устройства следва да се инсталират антивирусни решения за откриване и блокиране на зловреден софтуер, като се гарантира по-високо ниво на защита срещу злонамерени дейности.

Редовното архивиране на данни и цялостният план за възстановяване след киберинцидент са от решаващо значение за МСП за минимизиране на времето за престой и загубата на данни в случай на кибер инцидент. Предприятията от сегмента следва редовно да архивират критични данни за сигурни местоположения и да тестват своите процедури за архивиране и възстановяване, за да гарантират целостта и наличността на данните. Също така, жизненоважни са периодичните одити и оценки на сигурността, за да се

идентифицират уязвимостите и слабостите в системите и процесите. Тези одити могат да се извършват вътрешно или чрез ангажиране на външни експерти по киберсигурност. Редовните одити помагат да се идентифицират областите за подобрение и да се гарантира постоянна ефективност на сигурността.

МСП могат да си партнират с MSSP, за да увеличат своите възможности за киберсигурност. MSSP предлагат специализиран експертен опит в областта на сигурността, денонощно наблюдение и услуги за откриване на заплахи, което позволява на МСП да се възползват от модерни технологии за сигурност и квалифицирани специалисти, без да са необходими значителни инвестиции във вътрешни ресурси.

Ключово е предприятията от сегмента да участват активно в инициативи и форуми за споделяне на информация за киберсигурността. Тези платформи предоставят ценна информация за възникващи заплахи, тенденции в атаките и най-добри практики, споделени от общността за киберсигурност. Бивайки информирани, МСП могат проактивно да адаптират своите мерки за сигурност, за да се противопоставят на най-новите заплахи. Специфичните за индустрията мрежи и асоциации за киберсигурност могат да осигурят на МСП подходящи за индустрията насоки, показатели и възможности за работа в мрежа. Присъединяването към тези асоциации позволява на МСП да се учат от други подобни бизнеси, да споделят опит и да получат ценна информация за специфичните за сектора предизвикателства и решения за киберсигурността.

Киберсигурността трябва да бъде инициатива отгоре надолу, като лидерите активно демонстрират своя ангажимент към киберсигурността. Ръководителите трябва да дават приоритет на киберсигурността, да разпределят подходящи ресурси и да дават пример в спазването на политиките и практиките за сигурност. МСП трябва да инвестират в текущи програми за обучение и образование на служителите, за да насърчат култура на киберсигурност. Това включва редовни обучения, семинари и кампании за повишаване на осведомеността, фокусирани върху текущите кибер заплахи, безопасно онлайн поведение и докладване на подозрителни дейности. Важно е лидерите редовно да съобщават на своите служители актуализации на киберсигурността, промени в политиката и най-добри практики. Кампаниите за осведоменост чрез имейли, бюлетини и канали за вътрешна комуникация спомагат за поддържането на киберсигурността в челните редици на

съзнанието на служителите и укрепват културата на сигурност. Наред с това, ключово е да се установят ясни механизми за докладване, чрез които служителите да съобщават за инциденти със сигурността, потенциални уязвимости или подозрителни дейности. Насърчаването на отворена култура на докладване гарантира, че инцидентите със сигурността се адресират своевременно, минимизирайки потенциалните щети и позволявайки проактивни мерки за реагиране.

МСП трябва да са наясно с приложимите разпоредби за защита на данните и поверителността, като Общия регламент за защита на данните (GDPR) в Европейския съюз или Калифорнийския закон за защита на личните данни на потребителите (CCPA) в Съединените щати. Спазването на тези разпоредби помага на МСП да защитят данните на клиентите и да избегнат потенциални правни и финансови последици. Съгласно тези нормативни рамки следва да се прилагат мерки за поверителност, като криптиране на данни, контрол на достъпа и минимизиране на данните, за да защитят данните на клиентите и служителите. Защитавайки личната информация и чувствителните данни, МСП могат да запазят доверието на заинтересованите страни и да намалят риска от злоупотреба с данните.

Редовните оценки на риска и одитите за съответствие помагат на МСП да идентифицират пропуски в прилаганите мерки за сигурност и да гарантират спазването на приложимите разпоредби. Тези оценки позволяват на МСП проактивно да се справят с уязвимостите и да подобрят позицията си на киберсигурност по структуриран и систематичен начин.

Когато става дума за организационна киберсигурност, редица ръководители на малък бизнес неусетно си въобразяват, че не са толкова податливи, колкото са големите компании. В действителност обаче големите компании могат да инвестират в по-стабилна архитектура за сигурност, която затруднява злонамерените кибер участници да се насочат към тях, с изключение на хардкор престъпниците. Всъщност проучванията показват, че по-малките компании са три пъти по-склонни да бъдат обект на кибератаки, отколкото по-големите. МСП обаче се възстановяват най-бавно, като се има предвид, че им липсва инфраструктурата и професионалният капацитет, с които разполагат по-големите организации.

Още една област, в която МСП изостават, е тази на чистата структура – един по-малък бизнес може да няма толкова пари или човешки капацитет, за да се конкурира с по-големите. Въпреки това, с по-издръжливите структури идва и по-голяма защита срещу и устойчивост на прекъсвания, особено тези, които засягат архитектурата за информационна сигурност.

Кибер рисковете представляват сериозен бизнес проблем. Много лидери на МСП все още трябва да премахнат изолираната перспектива, която третира кибер рисковете като уникален проблем, отделен от това как работи бизнесът. Подобен възглед е създал изолирани ИТ отдели, където никой друг наистина не знае как работи нещо и грешките са неизбежни. Лидерите с тази гледна точка също е вероятно да считат киберрисковете просто за проблем с парите или инфраструктурата. Поради това те продължават да купуват оборудване и софтуер, които не са правилно интегрирани в бизнес процеса.

На този етап е жизненоважно да се каже, че киберсигурността е сложен проблем, където повечето предизвикателства категорично не могат да бъдат сведени до един фактор. Посрещането на нуждите на МСП от информационна сигурност изисква цялостна перспектива, при която всеки фактор консолидира другия. Така че, въпреки че наистина може да има случаи, в които е необходимо по-добро оборудване, лидерите трябва да обмислят как новите фантастични инструменти се справят с начина, по който правят бизнес в момента.

Когато компанията третира киберрисковете като бизнес проблем, нейните лидери започват да откриват защо е важно да им обръщат внимание и да ги третират като предизвикателства за заседателната зала, каквито са. Така самите лидери целенасочено придобиват значителни познания за ландшафта на информационната сигурност и определят най-големите потенциални заплахи за техния организационен модел. Това не означава, че решенията трябва да се издават като механични инструкции – напротив, лидерите и управленският персонал трябва да предоставят насоки за компанията по отношение на киберзащитата. Тази посока е уникална за всеки бизнес, в зависимост от неговия характер, размер, финанси, местоположение и други фактори.

Тъй като киберпрестъпниците се възползват от слабите инфраструктури за сигурност на малките и средни предприятия, за да стартират смъртоносни, неочаквани атаки, те по-конкретно експлоатират някои действия на служители и доставчици на трети страни, за да отправят вътрешни заплахи към малкия бизнес. Тези заплахи възникват, защото хората в организациите са или небрежни, или злонамерени. И двата фактора разкриват по-дълбока грешка в структурата на информационната сигурност, която предпоставя уязвимост в киберсистемите поради липса на контрол с нулево доверие.

Практически всяко МСП има някаква форма на контрол на киберсигурността, но в повечето случаи е необходимо да се извърши пълномащабна оценка и преработка, ако стратегията е фокусирана единствено върху външни рискове. За да се борят с вътрешните заплахи, предприятията от сегмента трябва да провеждат цялостно обучение по киберсигурност за служителите си, да налагат стриктни политики и контрол за киберсигурност и да са проактивни в наблюдението на това, което влиза и излиза от вашите системи. Подобно на веригата, една компания не може да бъде по-силна от най-слабото си звено.

Няма подход към киберсигурността, който да бъде успешен днес, без да се ръководи от данни. Способността да се обхване с един поглед какво работи и какво не е подценявана сред бизнес лидерите днес, особено що се отнася до киберсигурността. Събирането на информация за заплахи в реално време е доказан начин за постигане на значително смекчаване на кибератаките. Главният изпълнителен директор с кибернетично съзнание е проактивен, а не реактивен, а използването на данни помага на този ръководител помага да стигне до целта си – подобрена киберсигурност на неговото предприятие – по-бързо. Това включва генериране на отчети в системите на компанията с цел намиране на модели и вратички, които могат да изложат бизнеса ви на риск, както и възможности за повишаване на текущите нива на киберсигурност.

Въпреки че големите корпорации се появяват най-много новините, МСП са истинските стълбове на местната и глобалната икономика. Като такива, нарушенията на киберсигурността, засягащи МСП в мащаб, могат да имат катастрофални последици за обществото. Нещо повече – 60% от МСП, претърпели кибератака, не се възстановяват и затварят в рамките на шест месеца, което е показателно за това каква опасност

представляват киберпрестъпленията за сегмента на малкия бизнес, ако този модел се възпроизведе в мащаб. Ето защо е ключово лидерите да подготвят бизнеса си да бъде по-силен в лицето на предизвикателствата, които в крайна сметка могат да бъдат избегнати.

V. СПРАВКА ЗА ПРИНОСИТЕ В ДИСЕРТАЦИОННИЯ ТРУД

Дисертационният труд извежда следните научни и научно-приложими приносни моменти, които имат както теоретичен, така и практико-приложен характер:

1 Теоретично е обогатено понятието „киберсигурност“, като авторът предлага комплексна, интердисциплинарна дефиниция на киберсигурността, която надхвърля чисто техническия подход. Тя се разглежда като организация на ресурси, процеси и структури за защита на киберпространството от събития, които не съвпадат с правата на собственост. Този подход интегрира правни, икономически, социални и технически аспекти, което го прави ценен теоретичен принос.

2 Идентифицирани са специфичните рискове и уязвимости на българските МСП. Чрез анализа са систематизирани и категоризирани ключовите заплахи за МСП (напр. ransomware, фишинг, злонамерен софтуер), като е акцентирано върху факторите, които ги правят особено уязвими - ограничени финансови и човешки ресурси, ниска дигитална култура и липса на специализиран персонал.

3 Разработена е цялостна четириетапна методика за повишаване на киберсигурността. Това е основен научно-приложен резултат. Методиката обхваща:

- **Етап 1**: Идентифициране и оценка на риска (финансов, пазарен, сигурност).
- **Етап 2**: Законодателни инициативи на национално и ЕС ниво.
- **Етап 3**: Институционални реакции и механизми за реагиране при инциденти.
- **Етап 4**: Конкретни действия за всички заинтересовани страни (МСП, банки, институции, клиенти).

Тази структурирана рамка предлага ясен и приложим път за предприемане на действия.

4 Проведено е оригинално емпирично изследване, което сравнява нагласите и разбиранията на два ключови сегмента. На първо място потребителите на услуги на МСП и на втора собственици/мениджъри на МСП. Резултатите показват нивото на осведоменост, предразсъдъци и очаквания от двете страни, което е ценна информация за разработването на целеви политики и кампании.

5 Изведени са конкретни препоръки за всички заинтересовани страни. На базата на целия анализ дисертацията предлага много конкретни, практико-ориентирани препоръки, адресирани към:

- МСП, чрез въвеждане на многофакторно удостоверяване, обучение на персонала, криптиране на данни, разработване на планове за реагиране.
- Държавни институции, чрез хармонизиране на законодателството, подобряване на институционалното сътрудничество, насърчаване на публични кампании за повишаване на осведомеността.
- Банки и финансови институции, чрез подобряване на сигурността на транзакциите и комуникацията с клиенти.
- Потребители, чрез поведенчески модели за по-безопасно онлайн пазаруване.

VI. ИЗПОЛЗВАНА ЛИТЕРАТУРА

1. Cavelty, M. D. 2010. Cyber-Security. In J. P. Burgess (Ed.), The Routledge Handbook of New Security Studies: 154-162. London: Routledge.
2. Chang, F. R. 2012. Guest Editor’s Column. The Next Wave, 19(4): 1–2.
3. Chapman, A., & Smith, R.G. (2001). Controlling financial services frauds, Trends and Issues in Crime and Criminal Justice, 2: 189, Australian Institute of Criminology, Canberra
4. Council of Europe. (2003). Additional protocol to the convention on cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through

computer systems (ETS 189), http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm последно посетен на 23.01.2024

5. Coventry, L., Briggs, P., Blythe, J., & Tran, M. (2014). Using behavioral insights to improve the public's use of cyber security best practices. Government Office for Science
6. Dimopoulos, V., Furnell, S.M., Jennex, M. & Kritharas, I. (2004) Approaches to IT Security in Small and Medium Enterprises, in Proceedings of the 2nd Australian Information Security Management Conference 2004, Perth, Australia
7. Doherty, N.F. & Fulford, H. (2006) Aligning the Information Security Policy with the Strategic Information Systems Plan, Computers & Security, 25(2), 55-63
8. Dojkovski, S.; Lichtenstein, Sharman; and Warren, Matthew J., (2006) "Challenges in Fostering Information Security Culture in Small and Medium Size Enterprises", in preceding of 5 th European Conference on Information Warfare and Security, 1-2 June, 2006. National Defense College, Helsinki, Finland
9. Goodall, J. R., Lutters, W. G., & Komlodi, A. 2009. Developing Expertise for Network Intrusion Detection. Information Technology & People, 22(2): 92-108.
10. Grabosky, P.N., Smith, R.G., & Dempsey, G. (2001). Electronic theft: Unlawful acquisition in cyberspace, Cambridge University Press, Cambridge
11. Herhalt, J. (2011). Cyber-crime-A growing challenge for governments, KPMG Issues Monitor, 8: 1-24, https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-crime.pdf последно посетен на 23.01.2024
12. Hollman and S. Mohammad-Zadeh, "Risk management in small business," J. Small Bus. Manag., vol. 1, pp. 47–55, 1984 http://dx.doi.org/10.1108/09593840910962186 последно посетен на 22.01.2024
13. T. Union, "Series X: Data Networks, Open System Communications and Security: Telecommunication security - Overview of cybersecurity," pp. 2—-3, 2008.
14. IBM, https://www.ibm.com/downloads/cas/OJDVQGRY последно посетен на 23.01.2024
15. Jindrichovska, Irena. 2013. Financial Management in SMEs. European Research Studies 16: 79–96

16. Johnson, D.W. & Koch, H. (2006) Computer Security Risks in the Internet Era: Are Small Business Owners Aware and Proactive? In Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06), IEEE Society Press.
17. Kimball, R. C., Failures in risk management. New England Econ. Rev. 2000, January/February 3-12
18. KPMG (2013). Global eFr@ud Survey, KPMG Forensic and Litigation Services.
19. Madhava S.S.P., & Umarhathab, S. (Eds.), (2011). Information Technology Act and cyber terrorism: A critical review. Cyber Crime and Digital Disorder, Tirunelveli, India: Publications Division, Manonmaniam Sundaranar University.
20. Norris, G., Brookes, A., & Dowell, D. (2019). The psychology of internet fraud victimization: A systematic review. Journal of Police and Criminal Psychology, 34(3), 231–245
21. Ojala, Arto, and Hannakaisa Isomäki. 2011. Entrepreneurship and small businesses in Russia: A review of empirical research. Journal of Small Business and Enterprise Development 18: 97–119
22. Oxford University Press. 2014. Oxford Online Dictionary. Oxford: Oxford University Press. October 1, 2014: http://www.oxforddictionaries.com/definition/english/Cybersecurity последно посетен на 22.01.2024
23. Paul Ruggiero, J.F. 2011. Cyber Threats to Mobile Phones. https://www.uscert.gov/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf последно посетен на 20.02.2024
24. Verbano, Chiara, and Karen Venturini. 2013. Managing risks in SMEs: A literature review and research agenda. Journal of Technology Management & Innovation 8: 186–97
25. Wallinger, W., Alderson, D., & Doyle, J. 2009. Mathematics and the Internet: A Source of Enormous Confusion and Great Potential. Notices of the American Mathematical Society, 56(5): 586-599.
26. Zinnbaur, D. (2005). Internet governance priorities and practices, United Nations

UNIVERSITY OF NATIONAL AND WORLD ECONOMY

Department of "National and Regional Security"

IMPROVING CYBERSECURITY IN SMALL AND MEDIUM BUSINESSES IN BULGARIA

ABSTRACT OF DISSERTATION THESIS FOR AWARDING THE EDUCATIONAL AND SCIENTIFIC DEGREE OF "DOCTOR" in the scientific specialty "Economics and Management" (Economics of Defense and Security), professional field 3.8. Economics

Author : Ivaylo Hristoskov Iliev

Department : „ National and regional security ”

Scientific Head : Assoc . Prof. Dr. Noncho Ivanov Dimitrov

Department : „ National and regional security ”

Sofia, 2025

The dissertation work has been discussed and directed for defense by the Department of National and Regional security " at University of National and World Economy – Sofia .

The author on the dissertation work is a doctoral student on independent preparation at the same department. The research and developments presented in the dissertation were carried out at the University of National and World Economy - Sofia .

The dissertation work is of volume from 222 standard pages and contains: a list of abbreviations, a list of graphs and tables, an introduction, an exposition in three chapters, a conclusion, a list of contributions, a list of used literature and appendices.

The public protection on the dissertation labor will is consists of on 25. 11. 2025 in the hall "Scientific advice" of the University of National and World Economy – Sofia , open meeting on The scientific jury , appointed with order on The Rector of the UNWE.

The materials by the protection are on location on interested parties persons in the Science Directorate of the UNWE - Sofia and internet the page on The University (www.unwe.bg)

I. GENERAL CHARACTERISTICS OF THE DISSERTATION

Topic relevance

Small and medium-sized enterprises in Bulgaria are more from 95% of all economic subjects – this does this one type business " spinal pillar " of native This farm metaphor however , considering the scale , quite is not enough . Something more – small and medium business represents no only the whole skeleton , and also the vital organs on the Bulgarian economy .

The entrepreneurial climate in our country however , along with a number of others difficulties – financial , institutional , cultural – no provide on this one type enterprises the possibilities for calmly development and the necessary protection . While some from the others dangers however can very easy yes be overcome , accepted or managed , then this one from cybercrime is not among them .

Digitalization on the business is considered for strength before the pandemic from Covid-19. The restrictions caused from the necessity from fight against the virus however they transferred rapid-fire the bigger one part from life , both personal and professional , online . This , combined with the insufficient preparedness as on consumers (natural and legal persons) persons) on the Internet , as well as on institutions in Bulgaria , leads to significantly increase on cybercrime . Its victims already are everything more often ordinary citizens or small businesses , not goals institutions or big enterprises .

This quite no surprise – online and mobile trade , internet payments , cashless payments payments are already way on life no only for separate units or for the young people . Social media profiles networks and corporate website are basic tools for communication , which already are even in textbooks by marketing . Digital marketing is stands out as one from the most desired specialties for training and qualification , and online the services save on the business time and money .

Everything this however requires targeted actions in connection with the restriction on the harmful ones influences on cybercrime . It is necessary for companies yes protect as own you employees and sensitive information and data on customers and users you . For this however have

need from proactive assistance and both countries – the competent institutions and themselves users . This means high institutional efficiency and at least average level on culture on consumption , for sorry both missing in Bulgaria .

II. VOLUME AND STRUCTURE OF THE DISSERTATION

The dissertation work is of volume from 222 standard pages and contains: a list of abbreviations, a list of graphs and tables, an introduction, an exposition in three chapters, a conclusion, a list of contributions, a list of used literature and appendices. The bibliography consists of 198 literary sources.

The dissertation is structured in the following sequence:

LIST OF ABBREVIATIONS
LIST OF GRAPHS AND TABLES
INTRODUCTION
CHAPTER ONE - ESSENCE AND PROBLEMS OF CYBERSECURITY IN BULGARIA. DIMENSIONS OF THE DIGITALISATION OF SMALL AND MEDIUM BUSINESSES IN BULGARIA
1.1 Theoretical dimensions of cybersecurity. Conceptual framework.
1.2 Factors increasing the importance of cybersecurity in Bulgaria
1.3 Small and medium-sized enterprises in Bulgaria
1.4 Digitalization of small and medium-sized businesses in Bulgaria
CHAPTER TWO - METHODOLOGY FOR INCREASING CYBERSECURITY IN SMALL AND MEDIUM BUSINESSES IN BULGARIA
2.1 First stage – identification and management of risks for small and medium-sized businesses in Bulgaria related to digitalization
2.2 Second stage – legislative initiatives in support of cybersecurity
2.3 Third stage – institutional responses in the event of cybercrime
2.4 Fourth stage – prevention of cybercrime affecting small and medium-sized businesses in Bulgaria

CHAPTER THREE - APPROVAL OF THE METHODOLOGY THROUGH EMPIRICAL RESEARCH. ANALYSIS, PREVENTION AND POSSIBLE DIRECTIONS FOR CYBERSECURITY AFFECTING SMALL AND MEDIUM BUSINESSES IN BULGARIA

3.1 Rationale for the study

3.2 Presentation of the research results

3.3 Comment and analysis of the results

3.4 Possible ways to improve the cybersecurity of small and medium-sized businesses in Bulgaria

CONCLUSION

CONTRIBUTIONS

BIBLIOGRAPHY

APPLICATIONS

III. CONTENT AND RESULTS OF THE RESEARCH

INTRODUCTION

Cybersecurity is becoming a growing problem for small and medium-sized businesses worldwide – more and more attacks are being carried out by criminals who target businesses for the valuable information they hold, with the sole aim of selling the data for large sums on the black market.

Large organizations, of course, are not insured. However, they have significantly greater financial, human, and technological resources at their disposal, which can be beneficial when it is necessary to quickly limit the consequences of cyberattacks. The smaller resources they work with, including in terms of data sets and sensitive information, however, does not lead to better protection of small and medium-sized companies, nor does it divert the interest of criminals from them.

Alarming data from Forbes shows that cybercrime has increased sixfold during the pandemic. No one, not even celebrities, is safe – in fact, 130 Twitter accounts were compromised in 2020, including those of Elon Musk and Barack Obama. In the same year, the Marriott hotel

chain suffered a cyberattack, during which the data of more than 300 million hotel guests was leaked.

It is clear that despite their vast resources for protection, even the tech giants are failing to keep up with cybercrime. Small businesses, especially in developing economies with a host of other problems, are becoming even more vulnerable to attacks. They often lack the technological protections needed to protect themselves from attacks, nor do they have the resources to invest seriously in cybersecurity.

The logic of the perpetrators probably lies in the fact that the small size of the business does not mean the same limitation in financial or resource terms – that is, a small business can work with large sums of money and customer data just as much as a large one, but is less protected. Indeed, the majority of small and medium-sized businesses in our country do not have any plan or technology for cybersecurity protection – thus these enterprises become a convenient target.

Moreover, it may turn out that the threats to the cybersecurity of small and medium-sized enterprises come even from within, not due to malicious intent, but due to insufficient qualifications and unlearned (sometimes general) skills to detect and counter cyberattacks. Unfortunately, this is often true not only for ordinary employees (if any), but also for the owners and managers of small businesses themselves.

Ransomware attacks are among the most common cybersecurity threats facing small businesses today. They involve encrypting a company's data and holding it "hostage" until a ransom is paid. These attacks are rarely noticed until it's too late – they usually happen via email, via a link to a simple document. Since even a micro-business can handle a significant amount of electronic communication, most people only realize their mistake after they open the encrypted file. In most cases, they then pay the "ransom," even if it costs them several thousand leva, because they don't have the time and resources to restore the encrypted information or are trying to save money by not using a quality backup as part of their normal work protocol.

Phishing is undoubtedly the biggest and most popular cyber threat faced by small and medium-sized businesses. These attacks work by tricking the user into providing their personal information by sending an email that appears to be from a trusted source or website. No company, regardless of its size, is "immune" to these scams. There are many examples from Bulgarian reality

here, but in most cases they are related to social networks and/or banking information that is requested via email in a window that is a very exact copy of the real one. Only after the incident has occurred, when going back and taking a closer look, does the deceived realize their mistake.

Another relatively simple method of attacking small businesses is malware. These types of attacks work by infiltrating a computer through an email attachment or other backdoor and then executing without the user's knowledge. Once inside, malware can wreak havoc on digital files by changing settings and permissions, blocking specific programs from running, and spying on user activity. Malware is also commonly found on public Wi-Fi networks, where users are at risk of having their devices compromised if they visit an infected website or simply browse the wrong page.

Social engineering is a technique by which criminals trick people into providing sensitive information through various means – impersonating someone else, most often a representative of a company-potential partner or contractor. With the growth of popularity of social networks, social engineering has become increasingly widespread, and messages sent through these platforms may contain malware, which can steal the user's personal information.

One of the main concerns for small and medium-sized businesses is data theft. This crime occurs when hackers take personal information from employees through fraud or dishonest practices. By gaining access to an employee's email account, hackers can easily spread ransomware , phishing , and pharming attacks across the company's network.

Employees themselves often pose a significant security threat to businesses of all sizes. They leave data on USB drives, provide easy access to company files, use the same password for both personal and work accounts, and fall for phishing schemes that trick them into providing their login information. So, all too often, cybersecurity breaches in small and medium-sized businesses turn out to be the result of human error, not even malicious action.

This brief overview of the most common examples of cybercrime against small and medium-sized businesses and the focus on some of their specificities shows that preventing attacks through targeted measures is the best option. The best way for small businesses to protect themselves from cybercrime is to have a complete security plan – one that includes data loss

prevention, an incident response plan in place, a review of staff access privileges, and training employees on cybersecurity best practices.

And in connection with the above, we can point out that the main research problem that the dissertation examines is the cybersecurity of small and medium-sized businesses in Bulgaria and the need for coordinated actions to increase it.

This brings us to the subject of the dissertation, namely the specific cybersecurity problems faced by small and medium-sized businesses in Bulgaria. The subject of the study is precisely the enhancement and prevention applied in small and medium-sized enterprises in our country.

The following methods were used in the dissertation: analysis of literary and information sources, study of foreign experience, qualitative risk analysis, comparative analysis, case study analysis and empirical research and study of the attitudes and understandings regarding cybercrime and cybersecurity by consumers and owners and managers of small and medium-sized businesses.

The aim of the dissertation is to clearly outline the dimensions of the cybersecurity problems of small and medium-sized businesses in our country, along with their interrelationships with institutions and clients, and to provide recommendations for improving the situation for Bulgarian companies. In this sense, the following tasks can be formulated:

- to build a theoretical and normative framework and to analyze cybercrime;
- to develop methodological solutions and present good practices;
- conduct an empirical study to measure the attitudes and level of understanding of cybersecurity issues among both consumers and owners and managers of small and medium-sized enterprises;
- to provide specific recommendations for improving cybersecurity and the business climate in Bulgaria, based on the results of the empirical research and the developed methodological solutions .

The main thesis , which will is defends in the dissertation is that in Bulgaria , more than in better the developed Western European economies , cybersecurity on small and medium business is a problem that requires immediate coordinated actions from country on institutions , businesses

and consumers . Namely the lack them to moment worsens business the climate and prevents on the construction on durable relationships on trust between companies and customers right now .

In support on this statement are used row **literary and informational sources –** here is order specialized literature by the topic , statistically data from NSI, Eurostat , institutional statistics and statements , online and offline publications on experts by the topic .

The placed **restrictions** are related to the territorial range and valley on The research is based and focused on on state territories on Republic Bulgaria . The study is also limited to small and medium business and the specific Bulgarian context . This circumstance can yes limit the direct line applicability on the results and the developed methodology to big corporations or to SMEs in countries with drastically different normative base , institutional environment and culture on cybersecurity .

Users on the results and the developed methodology for increase on cybersecurity of SMEs in Bulgaria would were useful for several key groups . The main target group are the owners and managers on small and medium enterprises that can yes use the methodology for assessment , planning and implementation on adequate measures for cyber security in their companies , such as by this one way decrease the risk from financial and reputational damages . The state institutions and regulatory organs , such as for example The Ministry on electronic management , too are important user , so as the dissertation examines the normative base and calls for coordinated actions ; they can yes use the recommendations for improvement on the policies for cybersecurity , programs for support and information campaigns aimed at to the little one business . Organizations for support on business (such as branch chambers and associations) can yes include the results from research in educational institutions programs , seminars and consultations that provide on their own members . Except this , consulting companies and suppliers on services by cybersecurity can yes use the methodology and data from the empirical study for adaptation and improvement on their own products and services offered of SMEs. Finally , the academic community can yes uses the dissertation as theoretical and empirical basis for future research in the field on cybersecurity , economy and e-commerce governance in Bulgaria .

CHAPTER ONE - ESSENCE AND PROBLEMS OF CYBERSECURITY IN BULGARIA. DIMENSIONS OF THE DIGITALISATION OF SMALL AND MEDIUM BUSINESSES IN BULGARIA

1.1 Theoretical dimensions on Cybersecurity . Conceptual apparatus .

The term " cybersecurity " is subject on row academic and popular works that to big degree are considering the topic from certain point of view point . The concept is uses widely and its definitions are strongly context - dependent variables , often subjective and sometimes uninformative . There is a little literature for this what actually means cybersecurity and how it is deployed the phenomenon in different contexts . The lack on short , wide acceptable definition that yes captures multidimensionality on cybersecurity , potentially hinders technological and scientific progress , as strengthens mainly the technical view , at the same time dividing the disciplines that must yes act agreed for resolution on complex challenges in front of cybersecurity . For example , there is spectrum from technical solutions that support cybersecurity – despite this , these solutions alone by myself you no is deal with the problem . There is multitude examples and significant scientific work , which demonstrate the challenges related to organizational , economic , social , political and other human dimensions that are indissoluble related to efforts for cybersecurity [1]. Fredrik Chang , former director by research at the Agency for national security in the United States states , discusses interdisciplinary character on cybersecurity :

1.2 " *Science" for cybersecurity offers very opportunities for progress on basis on multidisciplinary approach , because in the end on the ends cybersecurity is fundamental connected with rivalry . People must yes protect machines that are attacked from others people using machines . So that , in addition to the critical traditional areas on computer sciences , electrical engineering and mathematics , are necessary prospects from others areas .*"[2]

[1] Goodall, JR, Lutters , WG, & Komlodi , A. 2009. Developing Expertise for Network Intrusion Detection. Information Technology & People, 22(2): 92-108.

http://dx.doi.org/10.1108/09593840910962186 last visited on 22.01.2024

[2]Chang, FR 2012. Guest Editor's Column. The Next Wave, 19(4): 1–2.

1.3 Cavalty notes that there is multitude interconnected discourses around the area on cybersecurity [3]. Deconstruction on the term cybersecurity helps yes is put the discussion in both areas of " cyber " and " security " and reveals some from the inherited problems . " Cyber " is prefix meaning cyberspace and refers to electronic communication networks and virtual reality [4]. He evolves from the term " cybernetics ", which is refers to the " *area" on the theory for control and communication , regardless whether in a machine or in an animal* " [5].

Faced with many definitions of cybersecurity from the literature, analysts need to follow a pragmatic qualitative research approach to support the definition process that merges objective qualitative research with subjective qualitative research. In effect, the result should be a tentative definition that is based on objectivity (e.g., an intrusion detection system) versus assumption (e.g., a hacker's intentions).

The absence on short , universal acceptable definition that yes covers multidimensionality on cybersecurity , hinders technological and scientific progress , as strengthens mainly the technical view for cybersecurity , such as at the same time divides the disciplines that must yes act agreed , for yes allow complex challenges in front of cybersecurity . It becomes everything more obviously that Cybersecurity is interdisciplinary phenomenon . The more comprehensive , unifying definition , there is for goal yes facilitate the interdisciplinary approaches to cybersecurity – one such definition follows yes be accepted from the multitude disciplines involved in the efforts for cybersecurity , such as by this one way can yes is achieve better understanding and cooperation needed for dealing with the growing and complex threats for cyberspace and the systems enabled from cyberspace .

1.2 Factors for increase the meaning on cybersecurity in Bulgaria

Computer and information systems revolutionize the mechanism for service by the whole world . The services offered on the individual and the community manually , disappear in favor on

[3] Cavelty , MD 2010. Cyber-Security. In JP Burgess (Ed.), The Routledge Handbook of New Security Studies: 154-162. London: Routledge.

[4] Oxford University Press. 2014. Oxford Online Dictionary. Oxford: Oxford University Press. October 1, 2014:

http://www.oxforddictionaries.com/definition/english/Cybersecurity last visited on 22.01.2024

[5] Wallinger , W., Alderson, D., & Doyle, J. 2009. Mathematics and the Internet: A Source of Enormous Confusion and Great Potential. Notices of the American Mathematical Society, 56(5): 586-599.

online services with the use on computer and internet technologies . Electronic training , electronic commerce , electronic business , and in the last time and electronic government transform traditional ways for work in virtual a world where " face to face " communication is happens , without yes you are face to face . Innovation , cost differentiation and growth , alliances and mergers are today's characteristics on the organizations that are possible thanks on digital revolution [6]. Despite all positive countries and opportunities that digitalization offers especially on small and medium business , active use on the new ones technology is related no only with social progress , but , especially in developing is economies , places on daily turn and question for cybersecurity and the increasing is Cybercrime . Dangers on the Web are one from the main ones reasons a number of SMEs in developing countries is countries everything will yes is feel unsure by attitude on the accession to online the community , which also explains the lower levels on digitalization on the private and the public sector in these economies .

Must yes is there is considering that cybercrime is criminal activity whose source is computer or computer network used for cyberattacks , and can yes includes fraud , theft , extortion , forgery and abuse , but because of the virtual regime is known to be difficult yes is detect and punish because of technical complexity and invisibility attackers who are sitting on thousands kilometers . Despite that the new ones technologies are comfortable , dynamic and developing and every next theirs level perfect functions and mechanism for security , due to nature on cybercrime and its ability to is develops with technology , is appear new threats with alarm the degree on regularity . So abilities on users yes you cooperate are upright in front of everything bigger challenges , which also can yes threaten security and financial health on all SMEs in the Network .

The problems arising from similar crimes , acquire big importance , especially those related to cracking , breaching on author's rights , children's pornography . They is they call more privacy issues when hackers / attackers attack confidential information , for yes do intentional distortions , yes stolen and intercepted legally or by other way . Despite that exists international legal system that is tries yes holds participants responsible for criminal deeds through The International punitive

[6]Madhava SSP, & Umarhathab , S. (Eds.), (2011). Information Technology Act and cyber terrorism: A critical review. Cyber Crime and Digital Disorder, Tirunelveli, India: Publications Division, Manonmaniam Sundaranar University.

court (ICC), the lack on coordination or incompatibility on local with international laws is becomes a barrier in front of hers success [7].

Online communication has become the norm in digital era , because of which internet consumers and governments are upright in front of elevated risk yes become victims on cyberattacks . Cybercriminals continuously develop avant-garde techniques , such as displace the goals yourself , focusing is less on theft on financial information and more on business espionage and access to government information . In context on quickly the disseminators is cybercrime governments in developing countries is countries must yes you collaborate in a global scale , for yes can yes is developed effective model for control on threats . Thanks on development and progress in computer and telecommunications technologies technologies , developing is countries are able yes develop and expand their own communication networks , such as them allow faster and easier networking and sharing on information . With this cybercrime is increase through the last several years in the world scale , which dramatically changes the scenario – in ours days the criminals use more complex devices , for yes break through cybersecurity . Something more , in the last years malicious software , spam emails , hacking on corporate websites and others attacks from this one character are case on computer " geniuses " , obvious from their talent .

These rarely malicious attacks gradually are is turned into unions for cybercrimes , draining money through illegal cyber channels . According to ratings only before decade about 2 billion users on internet and 5 billion mobile phones are related by the world . Everyone day is exchange about 294 billion email and 5 billion telephone messages [8]. Convenience on digital networks however there is price , so as business organizations in particular and societies as whole everything more rely on computers and the internet based networks , due to which cybercrime and digital attacks are is increased repeatedly by the whole world . The attacks are categorized as financial fraud , computer hacking , downloading on pornographic images from internet , viral attacks , persecution on electronic mail and creation on websites that encourage racial hatred [9]. The main

[7] Grabosky , PN, Smith, RG, & Dempsey, G. (2001). Electronic theft: Unlawful acquisition in cyberspace, Cambridge University Press, Cambridge

[8] Zinnbaur , D. (2005). Internet governance priorities and practices, United Nations

[9]. Herhalt , J. (2011). Cyber-crime-A growing challenge for governments, KPMG Issues Monitor, 8: 1-24, https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-crime.pdf last visited on 23.01.2024

and leading step to protection is better understanding on the different ones types threats , before which are upright business community and online users .

Often the ones encountered cybercrime include fraud with prior fee , explanation on botnet networks , failure from service (DoS) and distributed refusal from service (DDoS) , renewal fraud on names on domains , fake ads , hacktivism , theft on laptop or other hardware , theft on identity , IP theft , copying on information , phishing , software for fear , social media , spam , spyware software , unprotected wireless local networks (WLAN) and viruses attacks [10]. Experts are on opinion that some governmental agencies can also yes use cyberattacks instead of armed war as new means for leadership on war and this was reported in 2010, when Stuxnet (a computer virus) is used for execution on invisible attack on The Iranian nuclear program that had to yes deactivate Iranian centrifuges for enrichment on uranium . Carders Stealing Bank, which is also known as data for credit map , it's also big cybercrime , in which duplicated cards is use for towing on cash from ATMs or in stores [11].

Having considering the international character on cybercrime , it can yes is happened no only in the regions from where originates from , and yes includes others countries or regions . Therefore cybercrime is needs no only from strongly reacting , but also from international coordinated measures for control . By the same way the mechanism for investigation and reporting on these crimes must yes requires very resources .

Cybercriminals and their techniques continuously is change , which straightens governments and businesses in front of the big one challenge yes keep up with the constant development on the offenders . According to Slave Wainwright , Director on Europol , criminal investigations on cybercrime , identification and tracking on the origin on crime is not only complicated , but sometimes impossible because of the limitless you nature , which is one from the big ones challenges for the developer is a world that already tests shortage on technologies [12]. A number

[10]KPMG (2013). Global eFr@ud Survey, KPMG Forensic and Litigation Services.

[11]Chapman, A., & Smith, RG (2001). Controlling financial services frauds, Trends and Issues in Crime and Criminal Justice, 2: 189, Australian Institute of Criminology, Canberra

[12]Council of Europe. (2003). Additional protocol to the convention on cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (ETS 189), http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm last visited on 23.01.2024

experts in various parts on the world that cyberattacks and cybercrimes are profitable venture – in the cyber world hackers carry out organized crime , such as sell confidential stolen information .

The operation through software is often encountered way , through which hackers receive access to systems and sensitive information . The software for updating on users on networked machines it is also easy way for cybercriminals . By this one way the current ones tools and antivirus software can yes be very useful at the protection on the network and systems used from online users , so as the presenter antivirus program can yes detects , removes and protects machines and networks on the user from malicious software , etc. By the same way , users must yes be careful and yes avoid pirate software . Education and literacy can yes help better for prevention on cybercrime , so that the training for this how yes be used information systems and how yes you avoid or yes is you protect from criminals in cyberspace is a necessity , for yes can users clear yes understand most often the ones encountered hacker actions tactics , such as phishing , social engineering or eavesdropping on packages and others [13]. Education and awareness in the online users must yes passed long way , for yes them protect from very types cybercrime – the introduction on new technologies requires training no only for the use on the new ones systems , but also for the rights , obligations and responsibilities associated with the new machines .

By similar way the regulations and laws that manage electronic systems , you need yes be wide widespread , so that users yes are aware of the regulatory laws and measures for cybercrimes , introduced from their governments , as well as internationally plan . From other country , the bad and conservative system for investigation is also an obstacle in front of the electronic security , so as the professional incompetence and political interference with registration of the FIR, the system for investigation and the cumbersome procedures for delay in court system on the country slow down justice , as by this one way hinder the right one application on cyber laws . Other means for eradication on cybercrime is harmonization on the international cooperation and legislation – especially by attitude on the motivated from greed and cyberterrorists [14].

[13]. Herhalt , J. (2011). Cyber-crime-A growing challenge for governments, KPMG Issues Monitor, 8: 1-24, https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-crime.pdf last visited on 23.01.2024

[14]. Herhalt , J. (2011). Cyber-crime-A growing challenge for governments, KPMG Issues Monitor, 8: 1-24, https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-crime.pdf last visited on 23.01.2024

By time on the restrictions because of the spread of COVID-19 very small enterprises had to urgently yes passed to remote work , opening because of the above-mentioned reasons opportunities for the emergence on very cybersecurity issues , from workers using personal computers for work - related tasks , to reading on the cloud with a little or no IT staff or resources .

Cybercriminals can easy yes manipulate the little one business – these organizations no can yes say " no " to ransomware attacks , so as they don't have spare system for recovery on data if be attacked . Everything this again it is related to the limitations in financial means by which SMEs are forced yes is they can handle it .

Human error is the leading one reason for data abuse in the small business . The report IBM too so establishes that the compromised identification data are the most common way , in which cybercriminals initially attack the data on the company . So as the little ones enterprises no is focus on the training by cybersecurity , often again because of lack on finance , employees can easy yes be deceived yes fall on fraud with social engineering , malicious threats or sharing on data for input , sensitive data and other company and client information , so as no know what yes are looking for yes identify suspicious cyber activity [15].

So as cybercrime grows and progresses with each passed year , more importantly from it's always the little ones enterprises yes understand how these types attacks can yes influence on the operations them and yes undertake the correct ones steps , for yes is protect . The early discovery on violation on the data is from decisive meaning for the rescue on reputation on the company and damages amounting to on thousands , without themselves practices yes are exceptionally dear .

The best practices for cybersecurity on the little one business include :

- systematically training on employees – enterprises must yes are considering continuously training , for yes are good familiar all of them them employees with potential security vulnerabilities , for recognition and avoidance on fraud , creation on strong passwords and security on sensitive information for clients and companies ;

[15]IBM, https://www.ibm.com/downloads/cas/OJDVQGRY last visited on 23.01.2024

●updating on the software for security - the companies must yes use protective walls , antivirus software and antispyware programs , for yes guarantee that the sensitive data no can yes be easy accessible from hackers . These programs for security also require regular updates , for yes protect successfully from vulnerabilities , so that the managers of SMEs should regularly yes check the websites on the suppliers on software , for yes learn for upcoming corrections for security and others updates ;

●protection on the company's data – so as very abuses is happen because of error on the employees , they follows yes have access only to vital information for their specific position . The companies must yes are considering programs for storage on records requiring from employees correctly yes clear or archive files . The regular archiving on the data on all computers and deployment with system for recovery if the information must yes be extracted because of cyberattack with security cost less from ransom for the encryptor key . Segmentation on network is another way yes avoid sharing on data throughout network . By this one way if part from the network is compromised , no everything is gone because of segmentation .

●policies for protection on password – small enterprises and their employees must yes use strong passwords for everyone site , to which is enters daily . Passwords never no must yes is share between employees or yes is record where the others can yes them see . This is free practice that however can yes save SMEs a lot problems ;

●encryption on data – all data available through personal devices , computers or servers must yes be protected through appropriate encryption in case on attempts for unauthorized access . When the data are encrypted at rest , they are protected from review , except if the user no has the right identification data and code . This is very important for all regulated from HIPAA data ;

●multifactorial authentication – this one tool requires additional information for check , for example code for security , sent on your phone , for entering networks , systems and computers . Whenever possible , it is important yes is uses MFA. The inclusion his for email , VPN access , security wall and software access leads to safer system and again no costs additional money on the company ;

●cyber insurance coverage – cyber insurance can significantly yes help for the protection on the little one business from the potential extreme expenses that arise from set from cyberattacks and financial damage and the damages for reputation caused from breakthroughs on data . The processors on cyber claims are the people who yes direct the victims leaders on small businesses

by time on the stressful process and yes them help yes select suppliers who are carefully selected according to the specific ones needs and conditions on the enterprise .

Cybercriminals often use human vulnerability and psychological elements , for yes stolen identification data and yes receive unauthorized access . So as phishing and social attacks engineering are directed mainly to people , human factor continues yes be important element that a CISO must yes take considering , for yes protect the organizations you from cyberattacks . Most data abuse are caused from human mistake , negligence or lack on awareness , for example through simply click on wrong connection . So that it is usual employees yes increase the digital you footprint , without yes are aware of the related risks .

" People are the weakest cybersecurity unit . " – this negative characteristic on human nature is deep rooted in the industry for cybersecurity . As a result on this there is row obstacles in front of this yes there is purposeful , constructive discussion how better yes is include people in the processes on cybersecurity . For difference from technologies and technical processes however the people are fickle and unpredictable . The problem with human factor is complicated because by its essence suggests serious sociological , psychological and philosophical discussion [16].

In the fight against cyberattacks human intuition and creativity always will be decisive . By time on geopolitical voltage , for example , the analyzers by security can yes foresee human behavior , yes foresee criminal activities and yes understand why the threats is direct to specific organizations . Cybersecurity however no maybe not must yes be responsibility on one team or department – she must yes be shared responsibility throughout organization , as well as in its expanded ecosystem from partners , suppliers and customers .

So as the organizations perceive hybrid models on work and accelerate acceptance on the cloud , they become more susceptible on ingestion on accounts and others types scams . Here why is it important employees yes understand how cyberattacks can yes influence on their business and how yes is protect from the first day . The new employees must yes passed training for awareness regarding cybersecurity as part from the process on recruitment and adaptation . In addition , the training for awareness regarding security must yes be continuous process that yes covers big

[16]Coventry, L., Briggs, P., Blythe, J., & Tran, M. (2014). Using behavioral insights to improve the public's use of cyber security best practices. Government Office for Science

diversity from topics and examples for phishing , ransomware and attacks through social engineering .

Despite that the training by Security is useful and mandatory for employees not always use these knowledge without incentive for this . Some see gamification as potentially means for encouragement on actively participation in activities for cybersecurity , but this only by myself you no yes be effectively , if no real tools that yes it allow . The modern landscape on cybersecurity has become too broad and complex , for yes be understood only from people , so that the use on strategy for defense in depth can yes is show from essential meaning . Through modernization and automation of IT processes can It would be possible . yes is reduce and improve impact on human factor on cybersecurity [17].

The European Commission (2005) defines the meaning on the definition on The European union for SMEs in the following way : In a single market without internal borders , from essential measures in favor of of SMEs to is founded on general definition , for yes is improve their consistency and efficiency and to is limit the violations on competition . This is more more necessary , as is there is considering the wide interaction between the national measures and measures of the EU for assistance of SMEs in areas as regional development and financing on scientific research ... For the member states the use on The definition is voluntary , but The Commission them invites , together with the European investment Bank (EIB) and the European investment fund (EIF) yes it apply possible most widely . Despite the volume on the definitions of SMEs, there is trend yes is accept quantitative criteria , of first place criterion for number on the staff or number on employees as main determining factor at the categorization of SMEs. Also so within on this one compromise there is trend for definitions that is distribute beyond the borders on separate country in time when the economic interaction between countries is intense . Namely product on these definitions is the definition for SMEs, legitimized from The European union and which is uses from most researchers .

The economic literature contains big differences in definition on small and medium enterprises . Statistical agencies , international organizations , governments on independent

[17]Norris, G., Brookes, A., & Dowell, D. (2019). The psychology of internet fraud victimization: A systematic review. Journal of Police and Criminal Psychology, 34(3), 231–245

countries is appear with different definitions and categorizations for the enterprises that no reflect the differences between them . The different definitions of SMEs are rather arbitrary than the resemblance on the level and nature on the economic development . None unique , universal accepted definition for small and medium enterprises . The present criteria are suffered revision and always are in process on rating . None neither one from both consent , nor tendency to convergence by attitude on the definitions , even between international organizations that unite as members the same countries . The meaning on the definition of SMEs for politicians is consists in evaluating on the categories enterprises and their contribution to employment , gross internal product and others macroeconomic indicators , for guidance on efforts , policies , strategies for development and programs for assistance on small and medium-sized enterprises . For the definition of SMEs Use is especially quantitative indicators , criterion for size on employees and the economic criterion for the annual turnover and summation on economic results in financial reports . Quantitative criteria facilitate the categorization on the business by dimensions , but contain the disadvantage on the lack on confidence and the lack of on access to the reported data . The need is irreplaceable from inclusion on quality characteristics on the enterprises at sorting them in classes . SMEs are name according to criteria for dimensions , but the characteristics on management , structure on property and others immeasurable aspects them distinguish from the big ones enterprises easier than quantitative indicators .

The support of SMEs in the efforts them for digitalization includes welcoming on row critical needs . Access to financing is one from the most critical , so as SMEs often is need from support , for yes invest in initiatives for digitalization , covering expenses as hardware , software and training on employees . In addition , the programs for training and development on the skills are from essential meaning for the equipment on employees of SMEs with digital skills needed for the effective use on technologies . SMEs often they don't have the internal expert experience required for coping with complexity on digitalization , which does consulting and advisory services valuable resource . These services can yes guide SMEs in the choice on technologies , development on strategy and management on the risk , as guarantee more smoothly travel to digitalization , they however also cost quite a few .

The threats from cybercrime , global corruption and the fast technological changes are challenges for the companies implementing technologies on Industry 4.0. Enterprises must yes

respond on the standards for compliance , for yes guarantee that the activities on the organization are in accordance with the existing ones regulations . The standards for compliance follows yes is understand as as compliance with the legal ones requirements , as well as ethical standards . Compliance means execution on all obligations on The organization 's requirements which the organization must yes corresponds , includes the applicable legislation (laws , regulations , etc.) normative acts) and there is small freedom in this attitude . In addition , the organization follows yes answers on different voluntary obligations , such as industrial or organizational standards , codes , principles on good management , as well as social and ethical norms recognized in the organization .

CHAPTER TWO - METHODOLOGY FOR INCREASING CYBERSECURITY IN SMALL AND MEDIUM BUSINESSES IN BULGARIA

2.1 First stage – identification and management on the risks for small and medium business in Bulgaria related to digitalization

SMEs are more vulnerable compared to large companies by time on periods on economic and financial recession , as the reasons are superiors from their characteristics – difficulty at restructuring or reduction , low degree on diversification on activities , more fragile financial structure , dependence from external sources on financing . The pandemic crisis sharpen these vulnerabilities , SMEs respond late on the challenges , and the reasons for this are especially in the limited resources — specifically shortage on finance and small monetary buffer — gaps in expertise and vulnerabilities in relationships with customers and suppliers .

In business literature is indicates that the risks for SMEs in the welcome on the consequences from the economic crisis is founded on the lack on financial resources and the high price on capital , along with the shortage on administrative and technical opportunities .

The pandemic crisis sharpen the difficulties faced which are facing SMEs and determines the necessity from revaluation on this one sector considering the place and role that there is he in the Bulgarian economy , so as it is deep integrated into the economic and social structure no only on the country , but also Europe - we recall that in the EU SMEs represent 99.8% of the general

number companies , provide 65% of the working ones places and generate 53% of the added value . From other country , despite vulnerabilities , SMEs are more flexible and adaptable from the big ones companies (characteristics that can yes them allow yes react correctly and quickly by time on crisis), which is owes on their size , type on ownership and hierarchical structures , proximity to the persons taking solutions from customers and others interested countries , which allows yes is received valuable market information . In addition , the pandemic creates business opportunities in certain areas as electronic trade , deliveries and mobile applications with solid technological character . At the same time time however leads to significant changes in consumer behavior , one from which is the promoted focus on online shopping and activities at all . Here why the companies must yes is adapt to these changes (which probably will be irreversible), for yes offer new valuable offer based on innovative technological solutions through investments in digitalization .

For yes is cope with the challenges posed by from the COVID-19 crisis and the aftermath recession and, at the same time , yes is benefit from the opportunities that arose through this one period , SMEs should yes be more sustainable . Sustainability of SMEs includes creativity and innovation (such as entrepreneurial skills) for welcoming on needs on customers and trends on market . Despite this , she herself as whole is causes from sustainability on ecosystems on the enterprise – therefore the government support and public policies are from decisive meaning for sustainability of SMEs, for yes can generalization on the new ones technologies on their level yes stimulates their sustainable growth , for generalization on the new ones digital technology and application on different innovative tools on the fourth industrial revolution .

The limited financial resources , as well as the dynamic and at the same time fragmented market limit diversification on the operations and assortment provided from sector of SMEs, which significantly increases the risk from business failure because of bankruptcy on these companies [18]. In addition , in small enterprises the process on management , for difference from the bigger ones companies , often is ignores and has narrower scope , which also contributes for appearance on multitude threats for their activity . At the same time time Jindrichovska noted that financial condition on the little ones enterprises is directly and significantly affected from their owners [19].

[18] Ojala , Arto , and Hannakaisa Isomäki . 2011. Entrepreneurship and small businesses in Russia: A review of empirical research. Journal of Small Business and Enterprise Development 18: 97–119

[19] Jindrichovska , Irena. 2013. Financial Management in SMEs. European Research Studies 16: 79–96

The author indicates that among others personal aspects are most closely related to probability from bankruptcy on enterprises , which must yes is take considered in the model for assessment on the risk from bankruptcy . These specific characteristics on the activity on sector of SMEs mean that identification and measurement on their financial risk must yes be different from this in the big ones enterprises . The lack on resources allowing of SMEs to react quickly on internal and external threats , means that they must yes perceive the strategy for management on the risk in a larger degree from the big ones organizations [20].

SMEs are recognized for key engines on the economic growth and social development in the world scale , which contribute for more from 50% of taxes , 60% of GDP, 70% of technological innovations and 80% of the whole employment in central regions . The enterprises from the segment have inherent characteristics that them distinguish from the bigger ones companies , such as bigger flexibility in response on changes and more specialized in their abilities .

The digital transformation blurs the borders between industries , brings strategic and organizational changes and causes competitiveness on enterprises . Because of inadequate internal and external resources , limited access to externally knowledge and unclear innovative strategies compared to larger ones companies , many SMEs are is faced barriers to digitalization from technical , technological , organizational and legal aspects . Meanwhile continuously the changing is business environment after The Covid-19 crisis threatens sustainable presentation of SMEs, which them forces yes accept digital technologies , for yes is compete and to remain alive . This suggests that survival of SMEs will be upright in front of challenge without especially attention to the potential risks in one developing is technological era . The management on the risk is one from the main ones approaches for SMEs for dealing with uncertainty and achieving on operational success . Compared to the big enterprises , SMEs with scarce resources are upright in front of more difficulties when becomes question for management on The risk . The methods for management on the risks vary from bigger companies to small companies , as a result on this is what SMEs need yes perceive suitable strategies for management on the risk in accordance with own you

[20] Verbano , Chiara, and Karen Venturini . 2013. Managing risks in SMEs: A literature review and research agenda. Journal of Technology Management & Innovation 8: 186–97

characteristics . Everything more however missing understanding on the relevant strategies for management on risk , especially in the context on digital transformation .

On first place in context on the market risk can yes be indicated the multitude crises from different character , born from Covid-19 and these by the chain on supplies . The research show that the outbreak of COVID-19 has unfavorable effect on continuity on business . SMEs are predisposed yes suffer at such conditions because of its vulnerability to the fast ones changes on the surrounding them macroenvironment . As a result on this is from decisive meaning yes is perceive strategies for digital transformation , for yes is deal with interruptions in work and chain for supplies on the pandemic . Previous study shows that the covid-19 crises are consider for basic engines for SMEs yes redirect the business you from offline physical shops to online shops because of the cases on blocking . Some authors also so emphasize the meaning on digital transformation for mitigation on the risks by the chain on deliveries and delivery on Sustainability . Strategies as access to the network for open innovations through digitalization however can yes threaten survival of SMEs. Problems as loss on strength at negotiation over suppliers , unstable partnerships in coordination , loss on competitive competitive advantages would occurred in a large degree if be exposed on more uncertain global economic markets .

Risk is key factor in the economic life , so as people and companies they do irrevocable investments in scientific research and development on products , facilities and equipment , inventory and human capital , without yes know whether the future monetary streams from these investments will be sufficient for yes compensate debt and own capital [21].

Recently cybersecurity is becomes the main problem of IT technologies because of the meaning on this phenomenon in a series areas , among which the national security and the world commercial system . Cybersecurity is defined as " *totality" from tools , policies , concepts for security , safety measures for security , guidelines , approaches for management on risk , actions , training , best practices , beliefs and technologies that can yes is use for protection on the cyber environment and the organization and assets on the user* " [22]. The meaning on cybersecurity for specific Bulgarian institutions no can yes be neglected , so as each successful cyberattack against

[21]Kimball, RC, Failures in risk management. New England Econ. Rev. 2000, January/February 3-12

[22]IT Union, “Series X: Data Networks, Open System Communications and Security: Telecommunication security - Overview of cybersecurity,” pp. 2—-3, 2008.

them will there is huge effect on the national security on Bulgaria , for example as affect her economic stability . Managers on small business suffer from lack on knowledge and awareness on the importance on the tools for security , which influences directly on speed on acceptance on cybersecurity . Therefore can to be necessary understanding on this one current problem according to the point of view point on management .

In our days management on the risk is turns into a serious problem that usually affects the presentation of SMEs due to different reasons as lack on resources and deficit on mechanisms that would could yes support their activity by management on the risk in general plan . In addition , SMEs, like on the big ones companies , always are upright in front of different risks – the important thing is that their existence is more vulnerable in everyone moment because of the little one size on their financial and non-financial resources . Usually business the strategies demonstrate less attention to the consequences from management on the risk , while several strategic the move , like avoidance , control and cooperation , would could yes decrease uncertainty . Underestimation on the risks leads to unfortunate consequences that usually affect as both tangible and intangible assets and, even worse , they lead the business to bankruptcy [23].

2.2 Second stage – legislative initiatives in support on cybersecurity

Local laws for protection on data and scope

- Constitution of the Republic of Bulgaria (Art . 32 and Art . 34) – sets the basics on the main thing law on personal life ;
- General regulation for protection on data (GDPR) – the Data Protection Act applies together with GDPR for the purpose insurance on additional protection in cases where GDPR does not contains specific provision ;
- Law for protection on personal data – (PDPA) – the main law for protection on personal data in Bulgaria , GDPR applies ;
- Law for electronic messages – arranges public relations related to the implementation on electronic messages ; includes some provisions related with the protection on personal data ;

[23]Hollman and S. Mohammad-Zadeh, “Risk management in small business,” J. Small Bus. Manag ., vol. 1, pp. 47–55, 1984

- Regulations for the activity on The Commission for protection on personal data and its administration – CPDP – by-laws normative act .

Organs for protection on the data

- The Commission for protection on personal data (Commission);
- Inspectorate to The Supreme judicial council (the Inspectorate)

Sanctions and non-compliance on the provisions set out in the above- mentioned normative acts :

Administrative sanctions :

Applies GDPR . others violations on the provisions of the LPDP, which no are provided for in the GDPR, the Commission / Inspectorate can yes impose penalty amounting to up to 5000 BGN (2500 EUR). In again violation follows double sanction . According to the Personal Data Protection Act, the Commission can yes imposes fines and administrative measures , but no powers for forcibly execution . The execution on sanctions is performs by separately administrative production by The law for administrative violations and penalties .

Criminal sanctions :

Who creates , acquires for myself you or for another , brings or by other way distributes computer programs , passwords , codes or others similar data for access to informational system or part from her for the purpose execution on certain crimes under the Criminal Code (Art . 171 (3), Art . 319a, Art . 319b, Art . 319c or Art . 319d), grapes punishment deprivation from freedom to two years . When is announce personal data , classified information or other protected from the law secret and the violation no constitutes more severe crime , the punishment is deprivation from freedom to three years .

Others :

Third countries that suffer damages as a result on violation on the relevant legislation , can yes present claims for compensation .

Registration / notification / authorization

The requirement for registration on the administrators on personal data is deleted in accordance with GDPR and such registration already is not necessary .

The Commission supports the following registers :

- public register on the administrators and processors who have appointed DPOs;
- public register on the accredited certifying organs ;
- public register on the codes for behavior by Article 40 of the GDPR;
- internal register for violations of the GDPR and the Act and the measures taken measures under Art. 58, §2 of the GDPR;
- internal register for notifications for violation on security on personal data by Art . 33 and Art . 67 of the GDPR.

The Inspectorate supports the latest two type registers .

2.3 Third stage – institutional reactions in case on cybercrime

In Bulgaria cybersecurity and protection on personal data is regulate basically from the following legislative tools :

- The law for cybersecurity since 2018;
- The general regulation for protection on data (Regulation (EU) 2016/679) (GDPR), directly applicable in Bulgaria ;
- The law for protection on personal data since 2002 (last amended in 2019), which was revised in 2019 for application of GDPR.

The two legal frames is apply parallel . Their subject is related to the extent that the legislator has established formal mechanisms for cooperation between the supervisors organs by cybersecurity and the Commission for protection on personal data (CPDP) in cases where incident with security would also constituted a violation on security on personal data .

In Bulgaria The law for cybersecurity applies The Directive for security on networks and information systems (NIS Directive , Directive (EU) 2016/1148) with minimum derogations and deviations from the original text on The Directive . In addition , the Directive regarding the measures for high total level on cybersecurity in the Union (NIS Directive 2, Directive (EU) 2022/2555) has been published in the Official newspaper on The European union on December 27, 2022 and enters into force from from January 16, 2023. According to Article 41 of NIS

Directive 2 by 17 October 2024, the Member States members must yes transpose the normative act in the national you legislation , and laws for transposition is apply from October 18, 2024. On the same date The NIS Directive will be canceled .

The law for cybersecurity contains essential set from rules aimed at to solution on the problem of cybersecurity through holistic approach . He outlines the specific ones responsibilities and obligations that legal persons , regulatory authorities and authorities must yes comply with , and determines mechanisms for prevention and response in cases on cyberattacks and others incidents . The normative act identifies the main ones responsible institutions and their area on competence , introduces the category operators on basic services and suppliers on digital services and determines their responsibilities and duties in connection with the necessary measures for security and procedures for notification on the relevant authorities in case on cybersecurity incidents .

Decision 192 of 09.04.2019 of The Ministerial advice foresees the creation on additional executive authorities responsible for network and information security in vital public sectors as energy , transportation , healthcare , supply on fresh drinking water and digital infrastructure . The solution also outlines the methodology and specific criteria for determination on the main ones public services , for which is apply the specific normative requirements .

The law for cybersecurity determines the specific powers on regulatory authorities responsible for insurance on compliance on the law , as for example Council for cybersecurity . He defines clear and detailed rules regarding hierarchical position , cooperation and communication with others state authorities , such as SANS, the Minister on defense and the minister on internal Cooperation and coordination between different state institutions are basic mechanisms for development on safe and sustainable digital environment . Consequently on this The law for cybersecurity foresees the creation on National center for reaction at incidents in the area on the information security (CERT Bulgaria), as well as Sectoral departments for reaction at computer incidents security (Sectoral CSIRTs) and National unit for single contact for general monitoring on the problems on network and information security , as well as cross-border collaboration with others member states of the EU.

The law for cybersecurity foresees complete and entire application on The NIS Directive through acceptance on by-laws acts , such as Ordinance for minimal requirements for network and information Security 2019 Ordinance foresees the minimum specific requirements for network and information security , which the obligated persons , suppliers on substantial and digital services , public and regulatory organs and others suppliers on public services , you need yes observe in order to creation on sustainable and stable digital environment .

On EU level , Regulation (EU) 2019/881 of The European parliament and Council of 17 April 2019 on ENISA and on the certification on cybersecurity on information and communication technologies and Regulation (EU) No 526/2013 on cancellation establishes goals , objectives and organizational ENISA and framework related issues for the creation on European schemes for certification on cybersecurity for the purpose of insurance on adequately level on cybersecurity for ICT products , ICT services and ICT processes in the EU, as well as for the purpose of avoidance on fragmentation on the internal market by attitude on the schemes for certification on cybersecurity in the EU.

Narrow the related question for protection on personal data and relevant requirements for technical and organizational measures that must yes apply the administrators and processors , as well as the regime on notification applicable in case on violation on security on personal data , is regulate of the GDPR . local level The law suffers comprehensive change in 2019, for yes answers on the new one general regulatory frame and yes apply The Directive for protection on the data by attitude on law enforcement (Directive (EU) 2016/680).

The following specific legal areas are outside the general range on application on The law for cybersecurity and regulate from specific sectoral laws and regulations :

- communication and information systems for processing on classified information by the meaning on The law for protection on classified information (available) only on Bulgarian language here), which establishes legal requirements for protection on classified information from unauthorized access (including mode on notification at incidents with security). and detailed frame on the measures for security). The corresponding supervisory The body is the State commission by security on the information .

- networks and information systems on The Ministry on defense , Ministry on internal works , Agency , State Intelligence agency , State agency " Technical operations ", National Intelligence Service and National service for protection that not related to electronic administrative service and electronic exchange on documents between administrative The relevant authorities requirements for networks and information systems and their management and control are subject on conditions and procedures set out internally in these administrative organs .
- enterprises providing public electronic communicational networks and/ or services by the meaning on The law for electronic messages , which establishes specific legal requirements for protection on integrity and security on electronic communicational networks and services , privacy on messages , as well as for protection on users data , including mode on notification in case on security breaches or violations on integrity . The corresponding supervisory authority is the Commission for regulation on communications (CRC). In 2021, the Law for electronic messages was amended for the purpose introduction on the new ones obligations and requirements according to The Directive for creation on European code for electronic communications (Directive (EU) 2018/1972).
- suppliers on certification services by the meaning on Article 3, paragraph 19 of Regulation (EU) No 910/2014 of The European parliament and Council of 23 July 2014 concerning the electronic identification and authentication services for electronic transactions on the internal market and Directive for repealing 1999/93/EC, which also contains requirements for application on technical and organizational measures in connection with the provided confidential services , as well as mode on notification in case on security breaches or loss on integrity . The corresponding supervisory organ on local level is CRC.

In addition , according to requirements on The law for payment services and payment systems , suppliers on payment services that by principle no fall within the scope on The law for cybersecurity , you need yes apply specific measures for security and yes notify the supervisor authority in case on significant operational incident or incident with security . The corresponding supervisory authority is the Bulgarian folk bank .

The Council by cybersecurity is the main supervisory organ by the questions on cybersecurity in the Republic Bulgaria . The members his include 18 government employees , including eight ministers and leaders on the main ones organs for national security and law

enforcement . The Council functions as advisory and coordinating organ to The Ministerial advice and there is for task yes analyze risks and cyber threats , yes develops methods for counteraction and yes offers specific decisions . The prerogatives on Council also so include increase on the necessary expert capacity and development on the existing ones human resources , including technological , infrastructural , financial and organizational components . The Council by cybersecurity there is also the task yes created and proposed national strategy for cybersecurity and road safety map for her application .

The Council acts as coordinating organ between The Ministerial council , the national Unified unit for contact and the Council by security to The Ministerial advice . Except this is in charge of developing on national plan for management on cyber crises and harmonization on sectoral policies .

The National coordinator by cybersecurity is a person nominated from the Prime Minister , which performs important supporting role on Council by cybersecurity . The main his responsibilities include :

- preparation and offering on changes in the National strategy for cybersecurity and the applicable road map ;
- taking over on active role in development on The National coordination and organizational network for cybersecurity , along with measures for insurance on her reliability , security and sustainability ;
- taking over on active role in the creation and development on The National cyber situational center and coordination on actions and overall reaction at threats from cyber crises and threats from hybrid character ; and
- insurance on support in cases on cyberattacks or hybrid attacks .

The state Electronic agency management " is special administrative body that answers for the provision on electronic access to administrative services on the wide one public and controls the activity on others administrative bodies in this guideline . The Chairman on The state Electronic agency management " has big diversity from executive powers according to The law for electronic management , which are additionally expanded in the Act for cybersecurity . He answers for the conduct on the state politics by attitude on network and information security , there is powers yes issues methodical instructions and yes coordinates the application on the policies for network and

information security and can additionally yes certifies compliance on information systems implemented from administrative authorities , with the requirements for network and information security . The chairman is obliged yes exercises control on the administrations for compliance on these requirements .

2.4 Fourth stage – prevention on cybercrime affecting small and medium business in Bulgaria

SMEs rely on exceptionally very on critical for the business data – information for customers , offers , orders and data for payment – and on practice no can yes they work neither day without them . Here why companies , regardless from the size , you need regularly yes they do spare copies on the important ones you data as first key step from prevention on cybercrime and yes is assure that these archives are recent and can yes be restored . Doing this , the organizations guarantee that their business can yes continue yes functions after impact on flood , fire , physical damage or theft . In addition , if have spare copies on the data that can quickly yes be restored , not can yes be blackmailed from attacks of ransomware.

First step here is the identification on the main ones data – information , without which the business no would could yes functions . Usually this includes documents , photos , emails , contacts and calendars , most from which is store in just a few common folders on computer , phone , tablet or network . Regardless whether is find on USB memory , on separately device or separate computer , access to the archives on data must yes be limited , so that they :

- yes no are accessible for the staff
- yes no are constantly connected (physically) or through local network) with the device that contains the original copy .

Ransomware (and any other malicious software) often can automatically yes is move to attached repository , which means that each similar archiving also can yes be infected , leaving the company without spare copy , which yes is restore . For bigger sustainability the spare ones copies must yes is store on other physical and/ or virtually place , so that theft yes no led to loss on both copies – the solutions for cloud storage are cost-effective and efficient way for achievement on this .

A number of SMEs use cloudy storage by time on the daily you work , without even yes you give account for this - except if no they work with own email server , emails already is stored "in

the cloud " . The use on cloudy repository where supplier on services stores the data in its infrastructure means that the information is physical separated from the physical location . This type services also offer high level on availability . Suppliers can yes provide on the organization storage on data and web services , without to be necessary she yes invest in advance in expensive hardware . Most suppliers offer limited space for storage free and bigger capacity for storage for minimal expenses for the little one business .

No all suppliers on services are the same , but the market is relatively mature and most already are perceived row good practices for security . By passing significant parts from IT services on supplier , SME is benefit from specialized expertise , which the smaller ones organizations probably would is made difficult yes justify by attitude on the costs .

The fact is that in SMEs archiving very is often displaced from row others more important tasks , but most network or cloudy solutions for storage already allow yes is they do spare copies automatically – for example , when new files from certain type is recorded in certain folders . Using on automated archives no only saves time , but also so ensures that it is available the latest version on the files if the business there is need from them .

Many ready solutions for archiving are easy for setup and accessible as is there is considering the critical for the business protection that offer . When the management chooses solution , you need also so yes take considering how much data must yes be archived and how much quickly must yes there is access to the data after everyone accident [24].

Malicious software (known also as " malware ") is software or web content that can yes harm on organization . The most famous form on malicious software are viruses – self-replicating is programs that infect legitimate software .

The antivirus software that often is includes free in popular operating systems , you need yes is uses on all computers and laptops .. Smartphones and tablets can yes require different approach .

[24] Dojkovski , S.; Lichtenstein, Sharman; and Warren, Matthew J., (2006) "Challenges in Fostering Information Security Culture in Small and Medium Size Enterprises", in preceding of 5 th European Conference on Information Warfare and Security, 1-2 June, 2006. National Defense College, Helsinki, Finland

The download on applications for mobile phones and tablets must yes is happens only from approved from the manufacturer stores (such as Google Play or Apple App Store). These applications is check for yes provide definitely level on protection from malicious software . Employees on the company no it is good yes have rights yes download applications on third countries from unknown suppliers / sources , so as they no yes be verified . The accounts on the staff must yes have enough access required for execution on their role , with additional permissions (i.e. for administrators), given only on those who is need from them . When is create administrative accounts , they follows yes is use only for this one specific task , such as the standard ones consumer accounts is use for general work .

For all IT equipment (tablets , smartphones , laptops and personal computers) management must yes is assured that the software and firmware always are updated with the latest versions from developers on software , suppliers on hardware and vendors . The implementation on these updates is one from the most important things that SMEs can do yes do , for yes improve security . Operational systems , programs , phones and applications must yes be tuned on " automatically " update " when this is an option . In a given moment these updates already no yes are available (so as the product reach the end on maintained you life) – then must yes is consider the replacement with modern alternative [25].

Exceptional It is tempting to is use USB devices or memory cards for transfer on files between organizations and people – enough is enough, however only one user yes include by inattention infected stick (for example , a USB device containing malicious software), for yes devastate the whole organization . When devices and cards is share openly , it happens difficult yes is follow what contain , where are were and who used them . Can yes is reduce probability from infection through :

- blocking on access to physical ports for most users ;
- use on antivirus tools ;
- permission only approved devices and cards yes is use in your organization - and nowhere elsewhere

[25]Doherty, NF & Fulford, H. (2006) Aligning the Information Security Policy with the Strategic Information Systems Plan, Computers & Security, 25(2), 55-63

These directives follows yes become inseparable part from the company policy , for yes is prevent the exposure on the organization on unnecessary risks . Management can also so yes stimulates employees yes transfer files through alternative means as email or cloudy repository instead of via USB [26].

Mobile technologies already are essential part from the modern business , such as everything more data is store on tablets and smartphones – something more , these devices now are so much as powerful as traditional computers and, so as often leave safety on the office , they is need from more bigger protection from desktop the equipment .

Suitable complex PIN code or password , for difference from the simple ones , which can easy yes be guessed or extracted from social media profiles media , will hinder on the ordinary criminal yes received access to official phone . Very devices already include recognition on finger prints for lock , without to be necessary password . Despite this , these functions no always are activated .

On staff is more likely yes be stolen (or yes them lose) tablets or phones when are far away from the office or home . For happiness , the greater part from the devices include free web based tools that are priceless when it disappear . They can yes be used for :

- tracking on the location on the device ;
- remotely lock on access to the device (for yes is hinder on someone other yes it uses);
- remote deletion on the data stored on the device ;
- extraction on spare copy on the data stored on the device .

The setup on these tools on all devices on the organization can yes it seems daunting at first , but with the help of on software for management on mobile devices the setting to standard configuration can yes is happened to one click .

Without meaning what phones or tablets uses the company , it is important that you yes is support current by each time . All manufacturers (Windows, Android, iOS) release regular updates that contain critical updates for protection . This one The process is quick , easy and free , and the

[26]Johnson, DW & Koch, H. (2006) Computer Security Risks in the Internet Era: Are Small Business Owners Aware and Proactive? In Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06), IEEE Society Press.

devices must yes be tuned yes is update automatically , when possible . Management SMEs need yes is assured that the staff knows how much important are these updates and yes explain how yes them do employees , if necessary . Similar on desktop computers , in a given moment these updates already no yes are available , so as the device will reach the end on his/her own maintained a life in which moment must yes is consider the replacement with modern alternative .

Exactly as the operating ones systems on the devices on the organization , everyone applications also must yes is update regularly with adjustments from the developers on software . These updates no only will add new functions , but will also “ patch ” all open security holes . And by this one paragraph the management must yes is assured that employees know when the updates are ready , how yes them install and that it is important yes it do immediately .

When is use public Wi-Fi points (in hotels or cafes), none way easy yes is understand who them controls or yes is prove that she belongs to on whom you think it is. If officially device is connect with these points , someone other can yes received access to :

- this , on which the employee works while connected ;
- personal data for entrance , which very apps and web services support .

The simplest protective measure is the official devices no is connect to the internet through unknown points , and instead of this yes is uses mobile 3G or 4G network , which there is built-in protection . This means that can also yes is uses " tethering " (where the others devices as laptops share the same 3G/4G connection) or wireless dongle provided from the mobile network . Can also so yes be used virtual private networks (VPN) – a technique that encrypt the data before yes be sent by internet . If is uses VPN on third countries , will must the technical opportunity for configuration . It is important to is relies only of VPNs provided from reputable suppliers on services [27].

The official ones laptops , computers , tablets and smartphones will contain very from the critical for the business data – personal information on customers , as well as details for online accounts , to which there is access the company . From essential the importance is these data yes

[27] Dimopoulos , V., Furnell, SM, Jennex , M. & Kritharas , I. (2004) Approaches to IT Security in Small and Medium Enterprises, in Proceedings of the 2nd Australian Information Security Management Conference 2004, Perth, Australia

are accessible for management , not for unauthorized users . Passwords – when are used correct – are free , easy and effective way for prevention on access on unauthorized users to yours devices .

Can yes is password for lock on screen , PIN or other method for authentication (such as finger imprint or face unlock) . If is uses mainly finger imprint or face unlock , will is introduces password less often , so that the leaders can yes think for setting on debt a password that is difficult for guessing .

Password protection it's not just for smartphones and tablets . Management of SMEs should yes is assured that for the whole office equipment (laptops and personal computers) uses is product for encryption (like BitLocker for Windows) using of the Trusted Platform Module (TPM) with a PIN or FileVault (on macOS), for yes is start devices . Most contemporary devices have built-in encryption , but everything again can yes is impose encryption yes be enabled and configured .

If available given the option yes two-factor identification (known more as 2SV) for any of organizational accounts , she must yes be used – this adds big Quantity security on the price on no very additional efforts . 2SV requires two different the method to " prove " the identity , before yes can yes is uses service , usually password plus one other method . This can yes it is a code , it has been sent on certain smartphone (or code that was generated from reader on cards on bank), which must yes be introduced in addition to the password .

The responsible about IT policies in the organization specialist follows yes is assured that employees receive useful , easy for understanding information regarding the setting on passwords . They must yes are easy for remembering , but difficult for guessing from someone another . The staff also so must yes avoids the use on most often the ones encountered passwords that the criminals can easy yes IT systems alone by myself you no must yes require from employees yes share accounts or passwords , for yes you end the work – everyone user there is personal access to specific systems , and the given level on access is always the lowest necessary for execution on the work that go hand for hand with minimize the unnecessary exposure on systems , to which no is need from access .

The specialist who answers for this how is use passwords in the organization , can yes do row things that will improve security . The most important thing is that the staff will there is dozens

non -work related passwords that also must yes remember , so that the imposition on password access to service in the office must yes is requires , only if really you have need . When is use passwords for access to service , it's good to no is impose regular changes – they really must yes is change only when available suspicion that identification data for entrance are compromised .

It is also necessary so yes be provided storage , so that employees yes can yes record passwords for important accounts (such as email and banking) and yes them keep (but no with itself device). The employees can yes forget passwords , which means that it is necessary yes is think for tools , through which they easy can yes them reset themselves . SMEs can yes are considering the use on managers on passwords – this are tools that can yes create and store passwords , to which is receives access via a " master " password . So as the main one password protects all others , it is necessary to be strong , for example three random words .

One from the most common mistakes is the unchangeable on the passwords by default on the manufacturers with which is issue smartphones , laptops and others types equipment . The change must yes is happened before the devices yes be distributed on staff . Despite this is necessary regularly yes is check devices and software , especially for discovery on unchanged passwords by default [28].

CHAPTER THREE - APPROVAL OF THE METHODOLOGY THROUGH EMPIRICAL RESEARCH. ANALYSIS, PREVENTION AND POSSIBLE DIRECTIONS FOR CYBERSECURITY AFFECTING SMALL AND MEDIUM BUSINESSES IN BULGARIA

3.1 Justification on the study

3.1.1 Necessity of conducting empirical research

[28]Paul Ruggiero, JF 2011. Cyber Threats to Mobile Phones. https://www.uscert.gov/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf last visited on 20.02.2024

In the previous two heads were considered in detail row characteristics on cybersecurity and prerequisites for its deterioration in context of SMEs in Bulgaria . The exit from the national context , which litchi from everyone separate section , is inevitable , so as , from one country , Bulgaria is a full-fledged member state of the EU, and from other , cybercrime , considering the virtual character on the phenomenon , categorically exceeds geographical borders on countries and supranational associations . In addition , the fact that Bulgaria there is very wide and easily accessible internet infrastructure , but lags behind in institutional , legislative and any other other practically plan in measures for fight against cybercrime , does the country attractive target for cyberattacks . Geopolitical situation that is worsens because of conflicts on interests between East and West , characteristic for Bulgaria because of its geographical location and political and ideological past also are prerequisite for deterioration on cybersecurity , as well as for the impact of SMEs from the consequences from this .

The little one business there is less resources , but more flexibility by attitude on the taking on solutions – here why there is big probability the proposed above methodology , at least in the part that is refers to modeling on consumer behavior on employees and customers of SMEs to be fully applicable in our country . For yes become clear whether that 's right , it will be conducted empirically research that yes explore attitudes on the owners on small and medium business and their customers by cybersecurity issues . This is necessary for yes maybe , on basis on the results , yes is give recommendations for this how and in what way part yes is apply the researched above methodology .

3.1.2 Object and subject of research

Object on research are the dimensions on cybersecurity and cybercrime in context on small and medium business in Bulgaria , and the subject – the specific attitudes by the topic of promotion on cybersecurity of SMEs the owners on such type businesses and their customers .

3.1.3 Goals and objectives

The goal on the empirical research is to is conduct how much the methodology set out in second head from the present dissertation work is suitable for application in the conditions in Bulgaria . In this context can yes be formulated the following tasks :

- choice on method for research ;
- construction on toolkit and selection on sample ;
- conducting on the empirical research ;
- summary , presentation and commentary on the results ;
- formulation on approval on the methodology and recommendations for improvement cybersecurity of SMEs in Bulgaria .

3.1.4 Research method

The Chosen One method for a survey is a poll – the same thing map for the owners on businesses and for users , which will do the comparison on the results easier and more convenient . Usually , people no they love yes separate time for filling on research – here why the questionnaire map contains 15 closed the question , the first 5 of which collect demographic data . Participation in the study is voluntary and anonymous , which is also described in the study itself. home on the map (Appendix 1).

The samples with which will is works for the goals on the dissertation work , are too small , for yes can the study yes claims for representativeness . The questions however will be formulated so that the study yes be reliable . At the preparation on the questionnaire map will is we strive yes be reflected all possible options for answer , and where it is not certain that this is possible yes be complied with , will be included option " other (please specify in the blank) text). For yes avoidable refusal from filling on the poll because of certain question , nobody from them no yes be mandatory – respondents will have opportunity freely yes miss questions and yes can successfully yes finish the survey .

The study will is distributes through social network , and at reaching on the necessary number answers , the poll will be closed and hidden .

3.1.5 Groups to be included and their characteristics

Equally important for increase on cybersecurity of SMEs is the behavior on four key agents – themselves enterprises (through their managers and employees), users on the products and services them , institutions and banks (so as of now , at practice , SMEs no can yes exist without yes use the services them). On behavior on the second two no can yes is influence easy , but , for

account on this , users and representatives on the business are enough flexible , that real changes in their attitudes and actions can quickly yes bring to improvement the situation with cybercrime in the segment in our country . Here why is it important they yes be investigated .

3.1.5.1 Small and medium business product users

Practical everyone person buys goods and services from small and medium business , consciously or no . Online shopping is over part from everyday life , which leads to the question realize do you users what responsibilities have by attitude own you are this too on the merchants , from which buy , cybersecurity . Namely this follows yes is check through the empirical research – for the goals on the convenience at the processing on the results needed 50 are filled surveys , and then reaching on this one number answers the study will be closed .

3.1.5.2 Owners and managers of small and medium-sized enterprises

The owners and managers SMEs often have too very professional and social roles in the same moment and the difficult one task yes is deal with them in the conditions on lack on enough resources from different species . In everything more digitalized world , this opens place for serious gaps in the field on cybersecurity , which criminals and potential such in security notice – here why in the last years namely SMEs are becoming everything more common targets on such attacks . There are do you awareness for this and what measures would undertaken the owners on businesses will become clear from the survey 50 of them .

3.2 Commentary and analysis on the results

3.2.1 Similarities between the attitudes of consumers and owners and managers of small and medium-sized businesses

As already was specified above , the owners on small business are necessarily also users on the products and services on others such . In addition , so as is typical for SMEs freer , horizontal instead of emphasized vertical communication up and down by clear expressed hierarchical levels , small businesses remain close to the customers you and me mix with them daily . Here why it is not surprising that the answers on both groups you resemble so much very much .

Missing quite clear judgment for this what share in the private sector they have SMEs – this is evident as at users , as well as the owners on enterprises . To big degree the unawareness on the key role on segment in the economy , not only in Bulgaria , but also in European and global scale , can yes is show problem from point of view point on that , that underestimating own you meaning , small businesses underestimate the threats that arise for security them .

And at both groups there is clear understanding that cybersecurity is refers to everyone – as to individuals , as well as to enterprises , without meaning from their size . More specifically , this opinion among the owners on SMEs – all they are indicated this one answer . At users everything more is meet others options , for example the one that cybersecurity is refers only to the big ones The fact that SMEs remain close to the customers you can yes assist the change on this one attitude , if is use suitable communication techniques .

Online attendance is mandatory for small and medium business – so both users and owners think on enterprises from segment . Observes is strongly preference to the positive ones options for answer , which is refer to this how The network assists the presentation on businesses and them approaches to users them . And at both groups respondents abruptly falls the number answers at the negative options that is refer to that , that online the presence hides his own dangers , as for customers , as well as for the owners . All again , awareness on this at the owners of SMEs is better – this means that the enterprises are ready , at least psychologically in the face on the leaders you are , yes is try for protect users Are you . however resources and daily obligations them it allow is a matter of which the answer is rather negative .

On the question how prefer yes they are shopping , both groups distribute the answers you almost by equal between “ *online ”* and “ *and on the two the way "* , as preferences specifically to the physical objects are a little and, and at users , and at the owners of SMEs, come from the older ones respondents . Here why is it positive for the possibilities for improvement on cybersecurity , that the similarities at the answers on the next ones questions are more from the differences .

Both users and owners of SMEs benefit actively from the possibilities yes choose by several options for answer on the questions that is refer to this from what must yes is bother users and what must yes do businesses , for yes minimize cyber risks .

More users and more owners on businesses is bother from the expiration on bank information than from this on personal data . The owners on businesses very clear realize the necessity users yes are exceptionally careful when employee of their SMEs requested sensitive information . At users awareness also there is , but it is in many smaller degree than at the leaders .

All listed options for answer on the question What must yes make SMEs, for yes protect users you ?, represent measures , commented above in the methodological second head on the dissertation labor . Users understand good that all them in one or other degree are important . The owners on businesses however almost unanimously is agree that all proposed measures must yes be taken , for yes is guarantees cybersecurity on users and himself business – here is include as in-depth inspection on employees and minimal level on access on information , both pure technological measures and solutions as maintenance on current devices , systems and software and use on cloudy services , secure internet points for access and backup copies on The worrying fact is that both users and owners on businesses no realize all the way how important is it the use on sure points for access to Internet – that 's the least the indicated option and at both groups surveyed .

For the role on consumers in ensuring on cybersecurity and customers and owners of SMEs, they believe it is very important they yes are careful at this what kind information give for myself you online , yes use , by opportunity , virtual cards , yes be careful what websites visit , especially what is refers to dubious links .

Does impression here that at least people and from both groups choose payment with virtual cards – more is emphasizes on giving on minimum information on the Web and attention to the sites and the ones followed connections .

The attitudes to the work on the institutions also you resemble a lot and at both investigated groups – significant part from respondents they believe that authorities no they work by direction improvement cybersecurity of SMEs in our country . The opinion for banking there are many institutions similar – a little users they believe that they can yes guarantee security on the data them , as well as to these on enterprises , in the owners on businesses this are a little more representatives , but the general picture remains the same .

On practice , this is owes rather on common in our country belief that the institutions no work , as well as on the fact that from several years here on practice the use on banking services is absolutely mandatory as for the ordinary people , and for the owners on businesses . That is , the ones so or otherwise no they work , on all paragraphs , so that the assistance cybersecurity SMEs are no exception , and others are imperative yes be used , here why the worries for this what they can and what no can yes guarantee would caused too very superfluous , but for account on this everyday stress . Objectively looking at , recent incidents there is also the two front – both from the NRA and from DSK bank expired personal and other data on thousands Bulgarians .

3.2.2 Differences between the attitudes of consumers and owners and managers of small and medium-sized businesses

Differences in attitudes on both groups are very small , but , for account on this , they do seriously impression and show that , however close yes are users and owners on businesses , everything again development on independent activity leads to a change in thinking .

The most striking example are the answers on question 12, which is refers to this must do you yes be sanctioned employees of SMEs, if because of their actions the company suffered at cyber incident . In the first group everything again are 4 self-employed people found persons – they give answer " *no* ", but the majority users they believe that the punishment for workers is necessary . This suggests that no yes stand so things at the representatives on business – and indeed , the majority here no they think that must yes sanction employees You are here . the explanation is as follows : rightly so users they count on that those working in businesses , from which they are shopping products and services must yes are exceptionally careful and responsible when becomes word for the sensitive information with which they work , more more than the digital trace is increases with each passed day . They however no realize good in front of what challenges , among other things the more professional ones cybercriminals , are SMEs facing difficulties . Enterprises from the segment difficult find employees , so as often no succeed yes is compete with the big ones companies neither by attitude on strictly distribution on tasks , nor what is refers to the payment .

Here why , in most cases , in the small business they work or themselves his owners , or , together with them , exclusively close and trusted people . Here why , usually , cyber incidents are result from error on employees , not from maliciousness . If everything again is show the second , most owners of SMEs not is hesitate yes do the decisive one step and yes is part with the disloyal frame . The admission on involuntary errors however no is I am fixing. with sanctions – something more , the lack on punishments no means lack on will for dealing with the problem . It means use on others tools that will guarantee as loyalty on the employee in the long term plan , and cybersecurity on the business and its users . Here the open speaking for miss and the reason yes is arrive to him , for the damage that are were caused , the taking on responsibility from the business as whole , no only from one worker speak for maturity on the organization .

The other essential difference that mandatory must yes be indicated , is in the answers on the question From what yes is bother users of SMEs in attitude on their cybersecurity ? Not small part from the first group surveyed – namely customers – claims that place for worry There is none . From the business however no indicate this one option neither once . The reason is that the owners SMEs well understand cyber risks in the big you part and, with the available resources , are strive yes them manage optimal . This however becomes practically impossible at irresponsibly consumer behavior – if the customers no realize that cybersecurity – theirs and ours businesses , from which shopping – is a responsibility in equal measure degree and for both countries , for the representatives on the business will be very more difficult yes protect both countries .

3.3 Possible roads for improvement on cybersecurity on small and medium business in Bulgaria

The empirical research shows that the exhibited in second head on the dissertation labor methodology is completely applicable in Bulgaria , as is refers to her part with the actions that follows yes be undertaken from country of SMEs and users on their products and services . In fact , the leaders and owners on enterprises from the segment are often and consciously users on products and services from the same , mostly because know how much difficulties meeting one a little enterprise with limited you resources and this yes support similar businesses them carries emotionally satisfaction . This means that these people they think simultaneously as business

managers and clients , and from here follows the more careful and responsible attitude as to own them security , as well as to this one on colleagues , from which they are shopping .

In addition , the flexibility with which SMEs have , allows very easier yes is take solutions which one part from the processes and the necessary further actions in the field on cybersecurity yes stay within on the company and which one yes be transferred on external counterparties . The smaller ones enterprises have relieved procedures for financing on row activities , here why from the taking on decision that it is necessary budget for training on the staff to the realization on such no need yes pass months and years in transition on the proposal up and back down by multitude hierarchical levels . In small businesses personal communication is significantly stronger – this does easier the engagement on all employees with problems on cybersecurity and more freely reporting and discussion on suspicious messages , without fear from punishments , as in the big ones companies . It is also easier to disclose on malice and internal threats . Difficulties here however can yes come from that , that because of shortage on resources , especially at the beginning on everyone business , employees use for work and personal life the same devices . The solution is a specialist yes assess how can yes protect good the working part from the information .

Users , from his/her own country , are good informed and always more often realize how is it possible the data them , especially the bank information with increase on card and online payments , yes expired and what they can be the consequences from this . Very people from first hand they know that no can yes rely on banks yes returned quickly the lost sums , here why prefer yes be more cautious and alone yes take measures for protection , for example , yes use only virtual cards for online payments and yes check the merchant in advance . This significantly assists the efforts on the leaders of SMEs, but , of course yes , no cancels the necessity from the laying them . Something more – at everything the bigger one offering on goods and services , it is more likely that customers yes choose yes buy from these merchants (online and physical) who demonstrate concern for cybersecurity on the enterprise you and, by this one way , and for this one on users .

In Bulgaria , for sorry , and the authorities in the face on institutions , and banks , rather make it difficult The fight against cybercrime . The fact is that the GDBOP is care for easy road

for reporting on incidents in a specialized for this online portal . Missing however large-scale informational campaigns aimed at specifically to SMEs and consumers on their products and services . Investigations on banks at reported phishing attack are slow and uncertain , and the recovery on the stolen amounts becomes barely after several months in which the customers often are treated as scammers , not as suffered . This means that the methodology from second The chapter is inapplicable in our country in its part for inclusion on institutions and banks – it is a fact that banks is they try yes undertake actions , but they are rather part from their PR strategies , not consistent and purposeful campaigns .

The state institutions anyway no show commitment to the problems specifically of SMEs, despite that namely they represent more from 85% of Bulgarian private sector . Missing official communication on high level between banks and institutions – so becomes SMEs need to separate resources no only for recovery on the enterprise after cyber incident , and for reporting on one and the same something in different institutions and directly participation in various investigations , which leads to refusal from communication for row cyberattacks , and from here - to impossibility for identification the real ones scales on cybercrime against the little one business in Bulgaria and, accordingly , taking on adequate measures from country on authorities for its limitation . In addition , the legislation categorically lags behind from ingenuity on cybercriminals – so , in summary , the following measures and recommendations will be in accordance with the desire and will of SMEs and their users yes are looking for proactively solution on cybersecurity issues .

IV. CONCLUSION

In today's digital landscape SMEs are upright in front of growing challenges by attitude on cybersecurity . Despite the size you , they are valuable targets for cybercriminals because of the limited you resources and potentially weaker measures for security . SMEs, like on the bigger ones organizations , handle sensitive data and are upright in front of significant financial and reputational risks in case on violation on security on the data . For them is from decisive meaning yes admit the meaning on cybersecurity and proactive yes invest in protection on their own digital assets .

Exists often common wrong perception that SMEs do not are profitable goals for cyberattacks . Cybercriminals however are watching on the representatives on the segment as on

easy targets because of their potentially limited measures for security and resources . From essential It is important for SMEs to understand that no are immunized against cyber threats and we need yes undertake suitable measures for protection on its digital infrastructure .

The little ones businesses everything more often is confront targeted attacks directed to theft on valuable data , interruption on the operations or blackmail for payment on In particular , the attacks on ransomware , when which the attackers encrypt critical data and require payment , for yes restore access , become in the last years prevailing . SMEs should yes are aware of these threats and yes apply preventive measures for mitigation on the risks . They however often have limited budgets allocated for measures for cybersecurity , which does challenge yes is invest in stable solutions for security and specialized staff . This restriction them does attractive targets for cybercriminals . Finding on cost-effective solutions becomes from decisive meaning for SMEs for strengthening on the protection them .

The enterprises from the segment can yes they don't have internal experience in the field on cybersecurity , which makes it difficult development and implementation on effective strategies for security . Without the right one expert experience identification on vulnerabilities and implementation on suitable controls for security is becomes a challenge . SMEs must yes study opportunities as outsourcing or engagement with managed suppliers on services for security (MSSP), for yes overcome this one gap .

The employees have critical role in maintaining on strong practices for cybersecurity . Many small and medium enterprises however they don't have adequate programs for training on the staff you for awareness regarding security . Without appropriate training employees can yes become victim on phishing attacks or unconsciously yes participate in risky online behavior . SMEs should yes give priority on awareness regarding security and yes train employees you regarding the best practices .

SMEs often rely on suppliers and third parties countries for different services . These third countries however can yes introduce potential vulnerabilities in the ecosystem , here why for SMEs is from decisive meaning yes evaluate the state on cybersecurity on their own suppliers , yes create sure communication channels and yes apply contractual agreements for mitigation on the risks from third countries .

Cyber the threats continuously is develop and regularly is appear new techniques for attacks and vulnerabilities . SMEs can yes is make it difficult yes keep up with the latest trends and, accordingly , to adapt their own measures for security . Yes be informed and proactive at the observation on emerging threats are from essential meaning for SMEs, for yes support effective protection on cybersecurity . They must yes develop comprehensive strategy for cybersecurity that is in line with their business goals and inclination to risk , which yes outline the controls for security , procedures for reaction at incidents and the mechanisms for recovery in case on cyber incident . The presence on plan for reaction at incident helps yes is reduce to minimum impact on breakthrough and guarantees quick reaction .

SMEs need to yes give priority on the training for awareness regarding cybersecurity for all employees . It follows yes covers topics as recognition on phishing emails , creation on strong passwords and safe use on the company's resources . Regular trainings and campaigns for notification can significantly yes decrease the risk from human mistake and yes improve the overall position on security on the organization . In addition , it is necessary to be imposed stable control on access , for yes is limit unauthorized such to sensitive systems and data . This includes application on strong passwords , multifactor authentication and principles for at least privileges . Through restriction on access only to those who it require , SMEs can yes decrease the potential surface for attack and yes minimize impact from breakthrough .

SMEs need to yes support updated his/her own software and systems and immediately yes apply corrections for security and updates . The software without them can yes contains famous vulnerabilities that cybercriminals can yes use . The implementation on process for management on the corrections helps for protection against famous vulnerabilities and strengthens the position on security . The protective firewalls and antivirus solutions provide main layer on protection against different cyber threats . SMEs need to yes deploy stable such for monitoring and filtering on incoming and outgoing network traffic . In addition , the all devices follows yes is install antivirus solutions for detection and blocking on malicious software , such as is guarantees higher level on protection against malicious activities .

The regular archiving on data and the overall plan for recovery after cyber incident are from decisive meaning for SMEs for minimization on the weather for downtime and loss on data in case on cyber incident . The enterprises from the segment follows regularly yes archive critical data for

sure locations and yes test their own procedures for backup and restore , for yes guarantee integrity and availability on the data . Also so , vital are the periodic audits and assessments on security , for yes is identify vulnerabilities and weaknesses in systems and processes . These audits can yes is carry out internally or through engagement on external experts by cybersecurity . Regular audits help yes is identify the areas for improvement and yes is guarantees permanent efficiency on security .

SMEs can yes you partner with MSSP, for yes increase their own opportunities for cybersecurity . MSSPs offer specialized expert experience in the field on security , 24/7 monitoring and services for discovery on threats , which allows of SMEs to is benefit from modern technologies for security and qualified specialists , without yes are necessary significant investments in internal resources .

It is key that businesses from the segment yes participate active in initiatives and forums for sharing on information for cybersecurity . These platforms provide valuable information for emerging threats , attack trends and best practices practices , shared from the community for cybersecurity . Being informed , SMEs can proactively yes adapt their own measures for security , for yes is oppose on the latest threats . The specific for the industry networks and associations for cybersecurity can yes provide SMEs suitable for the industry guidelines , indicators and opportunities for networking . Joining to these associations allows of SMEs to is they study from others similar businesses , yes share experience and yes receive valuable information for the specific for sector challenges and solutions for cybersecurity .

Cybersecurity must yes be initiative from above down , like the leaders actively demonstrate his/her own commitment to cybersecurity . The leaders must yes give priority on cybersecurity , yes distribute suitable resources and yes give example in compliance on policies and practices for security . SMEs need yes invest in current programs for training and education on employees , for yes encourage culture on cybersecurity . This includes regular trainings , seminars and campaigns for increase on awareness , focused on current cyber threats , safe online behavior and reporting on suspicious activities . It is important that leaders regularly yes report on their own employees updates on cybersecurity , policy changes and best practices practices . The campaigns for awareness through emails , newsletters and channels for internal communication help for maintenance on cybersecurity at the forefront rows on consciousness on employees and strengthen

culture on security . In addition , it is key to is establish clear mechanisms for reporting , through which employees yes report for incidents with security , potential vulnerabilities or suspicious activities . The promotion on open culture on reporting guarantees that the incidents with security is address in a timely manner , minimizing the potential damage and allowing proactive measures for response .

SMEs need to yes are aware of the applicable regulations for protection on data and privacy , such as The general regulation for protection on data (GDPR) in the European union or Californian law for protection on personal data on consumer protection (CCPA) in the United States states . Compliance on these regulations helps of SMEs to protect the data on customers and yes avoided potential legal and financial consequences . According to these normative frames follows yes is apply measures for privacy , such as encryption on data , control on access and minimization on the data for yes protect the data on customers and employees . Protecting personal information and sensitive data , SMEs can yes keep trust on interested parties countries and yes decrease the risk from data misuse .

The regulars ratings on risk and audits for compliance help of SMEs to identify gaps in the applied measures for security and yes guarantee compliance on applicable provisions . These ratings allow of SMEs proactively yes is address vulnerabilities and improve the position you on cybersecurity by structured and systematic way .

When becomes word for organizational cybersecurity , a number leaders on small business imperceptibly you they imagine that no are so much as susceptible as are the big ones companies . In reality however the big ones companies can yes invest in a more stable architecture for security , which makes it difficult the malicious cyber participants yes is direct to them , except on hardcore criminals . In fact the studies show that the smaller ones companies are three times more inclined yes be object on cyberattacks than the larger ones . However, SMEs is restore slowly , as is there is considering that them missing infrastructure and professional capacity with which have the bigger ones organizations .

More one area in which SMEs lag behind is this on the pure structure – one smaller business can yes no so much money or human capacity , for yes is competes with the larger ones . Despite

this , with the more durable ones structures a bigger one is coming protection against and resistance on interruptions , especially those who affect the architecture for informational security .

Cyber the risks represent serious business problem . Very leaders of SMEs still more must yes removed the isolated perspective that treats cyber the risks as unique problem , separate from this how works business . Similar view has created isolated IT departments , where nobody other really no knows how works something and mistakes are inevitable . Leaders with this point of view point it is also likely yes consider cyber risks simply for money problem or the infrastructure . Because of this they continue yes buy equipment and software that no are correctly integrated into business the process .

On this one stage is vital yes is say that Cybersecurity is complicated problem where most challenges categorically no can yes be reduced to one factor . The reception on needs of SMEs from informational security requires comprehensive perspective , at which everyone factor consolidate the other . So that , despite that really can yes there is cases where it is necessary better equipment , leaders must yes are considering how the new ones fantastic tools is deal with the way in which which they do business at the moment .

When the company treats cyber risks as business problem , its leaders begin yes discover why is it important yes them turn attention and yes them treat as challenges for the meeting room hall , whatever are . So themselves leaders purposefully acquire significant knowledge for the landscape on the information security and determine the biggest potential threats for their organizational model . This no means that the decisions must yes is issue as mechanical instructions – on the contrary , leaders and management staff must yes provide guidelines for the company by attitude on cyber defense . This direction is unique for everyone business , depending from his/her nature , size , finances , location and others factors .

So as cybercriminals is benefit from the weak infrastructures for security on small and medium-sized enterprises , for yes start deadly , unexpected attacks , they more specifically exploit some actions on employees and suppliers on third countries , for yes send internal threats to the little one business . These threats arise because people in organizations are or careless , or malicious . Both the factor reveal deeper structure error on the information security , which assumes vulnerability in cyber systems because of lack on zero control trust .

Practical every SME has some form on control on cybersecurity , but in most cases it is necessary yes is carried out full-scale evaluation and processing , if the strategy is focused only on external risks . For yes is struggle with internal threats, businesses from the segment must yes are conducting overall training by cybersecurity for employees you are , yes impose strict policies and control for cybersecurity and yes are proactive in monitoring on that which enters and exits from yours systems . Similar on the chain , one company no can yes be stronger from the weakest you unit .

None approach to cybersecurity , which yes be successful today , without yes is lead from data . The ability yes is encompass with one look what works and what is not underestimated among business the leaders today , especially what is refers to cybersecurity . The collection on information for threats in real life time has proven way for achievement on significantly mitigation on cyberattacks . The main executive director with cybernetic consciousness is proactive , not reactive , and the use on data helps on this one leader helps yes arrive to the goal you – improved cybersecurity on his/her enterprise – faster . This includes generation on reports in the systems on the company with the aim of finding on models and loopholes that can yes expose the business you on risk as well as opportunities for increase on current level on cybersecurity .

Despite that the big ones corporations is appear the most the news , SMEs are the real ones pillars on the local and the global economy . As such , the violations on cybersecurity issues affecting SMEs at scale can yes have catastrophic consequences for society . Something more – 60% of SMEs suffered cyberattack , no is restore and close within on six month , which is indicative for this what kind danger represent cybercrime for the segment on the little one business if this one model is reproduced to scale . Here why is it key the leaders yes prepare the business you yes be stronger in the face on the challenges that ultimately account can yes be avoided .

V. CONTRIBUTIONS TO THE DISSERTATION

The dissertation brings out the following scientific and scientifically applicable contributions, which are both theoretical and practically applied in nature:

1 The concept of "cybersecurity" is theoretically enriched, as the author proposes a complex, interdisciplinary definition of cybersecurity that goes beyond a purely technical approach. It is viewed as an organization of resources, processes and structures to protect cyberspace

from events that do not coincide with property rights. This approach integrates legal, economic, social and technical aspects, making it a valuable theoretical contribution.

2 The specific risks and vulnerabilities of Bulgarian SMEs have been identified. The analysis has systematized and categorized the key threats to SMEs (e.g. ransomware , phishing , malware), with an emphasis on the factors that make them particularly vulnerable - limited financial and human resources, low digital culture and lack of specialized personnel.

3 A comprehensive four-step methodology for enhancing cybersecurity has been developed. This is a major scientific and applied result. The methodology covers:

- **Stage 1** : Risk identification and assessment (financial, market, security).
- **Stage 2** : Legislative initiatives at national and EU level.
- **Stage 3** : Institutional responses and incident response mechanisms.
- **Stage 4** : Concrete actions for all stakeholders (SMEs, banks, institutions, customers).

This structured framework offers a clear and actionable path for action.

4 An original empirical study was conducted that compared the attitudes and perceptions of two key segments. Firstly, users of SME services and secondly, SME owners/managers. The results show the level of awareness, prejudices and expectations on both sides, which is valuable information for the development of targeted policies and campaigns.

5 Specific recommendations are derived for all stakeholders. Based on the entire analysis, the dissertation offers very specific, practice-oriented recommendations, addressed to:

- SMEs, by introducing multi-factor authentication, training staff, encrypting data, developing response plans.
- State institutions, through harmonization of legislation, improvement of institutional cooperation, promotion of public awareness campaigns.
- Banks and financial institutions, by improving the security of transactions and communication with customers.

- Consumers, through behavioral patterns for safer online shopping.

VI. REFERENCES

1. Cavelty , MD 2010. Cyber-Security. In JP Burgess (Ed.), The Routledge Handbook of New Security Studies: 154-162. London: Routledge.
2. Chang, FR 2012. Guest Editor's Column. The Next Wave, 19(4): 1–2.
3. Chapman, A., & Smith, RG (2001). Controlling financial services frauds, Trends and Issues in Crime and Criminal Justice, 2: 189, Australian Institute of Criminology, Canberra
4. Council of Europe. (2003). Additional protocol to the convention on cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (ETS 189), http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm last visited on 23.01.2024
5. Coventry, L., Briggs, P., Blythe, J., & Tran, M. (2014). Using behavioral insights to improve the public's use of cyber security best practices. Government Office for Science
6. Dimopoulos , V., Furnell, SM, Jennex , M. & Kritharas , I. (2004) Approaches to IT Security in Small and Medium Enterprises, in Proceedings of the 2nd Australian Information Security Management Conference 2004, Perth, Australia
7. Doherty, NF & Fulford, H. (2006) Aligning the Information Security Policy with the Strategic Information Systems Plan, Computers & Security, 25(2), 55-63
8. Dojkovski , S.; Lichtenstein, Sharman; and Warren, Matthew J., (2006) "Challenges in Fostering Information Security Culture in Small and Medium Size Enterprises", in preceding of 5 th European Conference on Information Warfare and Security, 1-2 June, 2006. National Defense College, Helsinki, Finland
9. Goodall, JR, Lutters , WG, & Komlodi , A. 2009. Developing Expertise for Network Intrusion Detection. Information Technology & People, 22(2): 92-108.
10. Grabosky , PN, Smith, RG, & Dempsey, G. (2001). Electronic theft: Unlawful acquisition in cyberspace, Cambridge University Press, Cambridge
11. Herhalt , J. (2011). Cyber-crime-A growing challenge for governments, KPMG Issues Monitor, 8: 1-24,

https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-crime.pdf last accessed 23.01.2024

12. Hollman and S. Mohammad-Zadeh, “Risk management in small business,” J. Small Bus. Manag ., vol. 1, pp. 47–55, 1984 http://dx.doi.org/10.1108/09593840910962186 last visited on 22.01.2024
13. T. Union, “Series X: Data Networks, Open System Communications and Security: Telecommunication security - Overview of cybersecurity,” pp. 2—-3, 2008.
14. IBM, https://www.ibm.com/downloads/cas/OJDVQGRY latest visited on 23.01.2024
15. Jindrichovska , Irena. 2013. Financial Management in SMEs. European Research Studies 16: 79–96
16. Johnson, DW & Koch, H. (2006) Computer Security Risks in the Internet Era: Are Small Business Owners Aware and Proactive? In Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06), IEEE Society Press.
17. Kimball, RC, Failures in risk management. New England Econ. Rev. 2000, January/February 3-12
18. KPMG (2013). Global eFr@ud Survey, KPMG Forensic and Litigation Services.
19. Madhava SSP, & Umarhathab , S. (Eds.), (2011). Information Technology Act and cyber terrorism: A critical review. Cyber Crime and Digital Disorder, Tirunelveli, India: Publications Division, Manonmaniam Sundaranar University.
20. Norris, G., Brookes, A., & Dowell, D. (2019). The psychology of internet fraud victimization: A systematic review. Journal of Police and Criminal Psychology, 34(3), 231–245
21. Ojala , Arto , and Hannakaisa Isomäki . 2011. Entrepreneurship and small businesses in Russia: A review of empirical research. Journal of Small Business and Enterprise Development 18: 97–119
22. Oxford University Press. 2014. Oxford Online Dictionary. Oxford: Oxford University Press. October 1, 2014: http://www.oxforddictionaries.com/definition/english/Cybersecurity last visited on 22.01.2024

23. Paul Ruggiero, JF 2011. Cyber Threats to Mobile Phones. https://www.uscert.gov/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf last visited on 20.02.2024
24. Verbano , Chiara, and Karen Venturini . 2013. Managing risks in SMEs: A literature review and research agenda. Journal of Technology Management & Innovation 8: 186–97
25. Wallinger , W., Alderson, D., & Doyle, J. 2009. Mathematics and the Internet: A Source of Enormous Confusion and Great Potential. Notices of the American Mathematical Society, 56(5): 586-599.
26. Zinnbaur , D. (2005). Internet governance priorities and practices, United Nations