

МОНОГРАФИЧНА БИБЛИОТЕКА „ЗНАНИЕ И БИЗНЕС“, КНИГА 13, 2021
ISBN 978-619-210-058-2, ВАРНА, БЪЛГАРИЯ
MONOGRAPHIC LIBRARY “KNOWLEDGE AND BUSINESS”, BOOK 13, 2021
ISBN 978-619-210-058-2, VARNA, BULGARIA

Монографична библиотека „Знание и бизнес“, книга 13
Monographic library “Knowledge and business”, book 13

Искрен Таиров / Iskren Tairov

**ИНФОРМАЦИОННА СИГУРНОСТ КАТО ПРИОРИТЕТ НА
СИСТЕМИТЕ ЗА ЕЛЕКТРОННА ТЪРГОВИЯ**

**INFORMATION SECURITY AS AN ELECTRONIC COMMERCE
SYSTEMS PRIORITY**

2021

Издателство „Знание и бизнес“, Варна
Publishing house “Knowledge and business” Varna

This book or any part of it may not be copied or distributed electronically without the written permission of the author.

- © Iskren Tairov, author, 2021.
- © Publishing house “Knowledge and business”, 2021.

This monograph is indexed in RePEc
(<https://econpapers.repec.org/bookchap/kabmonogr/13.htm>).

ISBN: 978-619-210-058-2

Editorial board “Knowledge and business”

Prof. PhD Petko Shterev Iliev – Head editor, University of Economics Varna, Bulgaria

Assoc. Prof. PhD Svetlozar Dimitrov Stefanov – Deputy Head editor, University of Economics Varna, Bulgaria

Prof. PhD Julian Andreev Vasilev – Deputy Head editor, University of Economics Varna, Bulgaria

Assoc. Prof. PhD Anastasia Stefanova Konduktorova – Scientific Secretary, University of Economics Varna, Bulgaria

Prof. PhD Marin Todorov Neshkov, University of Economics Varna, Bulgaria

Assoc. Prof. PhD Pavel Stoyanov Petrov, University of Economics Varna, Bulgaria

Assoc. Prof. PhD Sabka Dimitrova Pashova, University of Economics Varna, Bulgaria

Assoc. Prof. PhD Desislava Borislavova Serafimova, University of Economics Varna, Bulgaria

Chief Assistant Prof. PhD Todor Kostadinov Dyankov, University of Economics Varna, Bulgaria

Chief Assistant Prof. PhD Svetlana Todorova, University of Economics Varna, Bulgaria

Prof. PhD Zdzislaw Polkowski, Uczelnia Jana Wyżykowskiego, Polkowice, Poland

Prof. PhD Stefan Bojnec, University of Primorska, Koper, Slovenia

Prof. PhD Young Moon, Syracuse University, Institute for Manufacturing Enterprises, USA

Prof. PhD Rajesh Khajuria, Gujarat Technological University, Ahmedabad, India

Dr. Amin Parag, SIES Colleague of Management Studies, Navi Mumbai, India

ИНФОРМАЦИОННА СИГУРНОСТ КАТО ПРИОРИТЕТ НА СИСТЕМИТЕ ЗА ЕЛЕКТРОННА ТЪРГОВИЯ

Искрен Таиров¹

¹Стопанска академия „Димитър Апостолов Ценов“, България
i.tairov@uni-svishtov.bg

Резюме

Обект на изследване в настоящия труд са системите за електронна търговия от тип бизнес към клиент (Business to customer - B2C) в българските компании. **Предмет на изследване** е информационната сигурност на тези системи, постигана чрез съвкупност от различни подходи, стратегии, методи, политики, техники и технологии.

Основната цел на изследването е, в съответствие с потребностите на съвременната икономическа теория и практика, да бъде извършено едно сравнително цялостно и систематизирано изследване на проблемите на информационната сигурност в сферата на електронната търговия. Така дефинираната цел се постига с решаване на следните **изследователски задачи**:

- изясняване на същността на *понятията информационна сигурност и защита* като основни компоненти на системите за електронна търговия;
- осъществяване на критичен анализ на съвременните *информационни и комуникационни технологии, подходи, решения и стандарти*, поддържащи защитена среда за функциониране на електронната търговия от тип бизнес към клиент;
- организиране и провеждане на *анкета* с участието на специалисти от практиката за установяване на текущото състояние на информационната сигурност в бизнес към клиент системите за електронна търговия на бизнес организациите в България;
- анализиране на *състоянието на информационната сигурност* в системите за електронна търговия от тип бизнес към клиент в български организации на база проведената анкета;
- изясняване на *подход за създаване на политика* за информационна сигурност и разширяване на рамката за информационна сигурност с нови елементи;
- разработване на *методология за политика и изграждане на модел* за информационна сигурност, който да е в съответствие със състоянието и потребностите на бизнес средата и технологичното обкръжение на български организации, осъществяващи електронна търговия.

На база на извършената изследователска работа и приложението на редица подходи, методи и анализи са постигнати следните научни и научно-приложни приноси:

- Изяснена е същността на понятието *информационна сигурност* и други, свързани с него понятия, а също така е извършен анализ на защитата като основен компонент на СЕТ.
- Направен е критичен анализ на съвременните *информационни и комуникационни технологии, подходи, решения и стандарти*, поддържащи защитена среда за функциониране на електронната търговия от тип B2C.
- Извършен е критичен анализ на база организирането и провеждането на анкета с участието на специалисти от практиката за установяване на текущото състояние на информационната сигурност в СЕТ от тип B2C на бизнес организации в България.
- Изяснен е подходът за създаване на *политика* за информационна сигурност и е разширена рамката за информационна сигурност с добавяне на нови елементи.

- Разработена е методология за политика и е изграден модел за информационна сигурност, който е в съответствие със състоянието и потребностите на бизнес средата и технологичното обкръжение на български организации, осъществяващи ЕТ.

Настоящата монография се базира на защитен дисертационен труд на 02.09.2015 г. в Стопанска академия "Д. А. Ценов"- Свищов на заседание на Научно жури.

Ключови думи: информационна сигурност, системи за електронна търговия, електронни транзакции, защитена среда, заплахи, мобилна търговия, измерения, технологични решения, организационни политики, протоколи за сигурност, индустриални стандарти, защитени електронни разплащания, методология за създаване на политика за сигурност, архитектурен модел на решение за информационна сигурност в системите за електронна търговия.

INFORMATION SECURITY AS AN ELECTRONIC COMMERCE SYSTEMS PRIORITY

Iskren Tairov¹

¹D. A. Tsenov Academy of Economics, Svishtov, Bulgaria
i.tairov@uni-svishtov.bg

Abstract

The object of research in this paper are the systems for e-commerce of business to customer (B2C) type in Bulgarian companies. The subject of research is the information security of these systems, achieved through a set of different approaches, strategies, methods, policies, techniques and technologies.

The main goal of the research is, in accordance with the needs of modern economic theory and practice, to conduct a relatively comprehensive and systematic study of the problems of information security in the field of electronic commerce. The goal thus defined is achieved by solving the following research tasks:

- clarifying the essence of the concepts of information security and protection as main components of e-commerce systems;
- Carrying out a critical analysis of modern information and communication technologies, approaches, solutions and standards, supporting a secure environment for the functioning of e-commerce of the business-to-customer type;
- organizing and conducting a survey with the participation of specialists from the practice of establishing the current state of information security in business to customer e-commerce systems of business organizations in Bulgaria;
- analysis of the state of information security in e-commerce systems of business to customer type in Bulgarian organizations on the basis of the survey;
- clarifying the approach to creating an information security policy and expanding the information security framework with new elements;
- development of a methodology for policy and construction of a model for information security, which should be in accordance with the state and needs of the business environment and the technological environment of Bulgarian organizations engaged in e-commerce.

Based on the performed research work and the application of a number of approaches, methods and analyzes, the following scientific and scientific-applied contributions have been achieved:

- The essence of the concept of information security and other related concepts is clarified, and an analysis of security as a main component of SET is performed.
- A critical analysis of modern information and communication technologies, approaches, solutions and standards that support a secure environment for the functioning of e-commerce type B2C.
- A critical analysis was performed on the basis of organizing and conducting a survey with the participation of specialists from the practice of establishing the current state of information security in SET type B2C of business organizations in Bulgaria.
- The approach to creating an information security policy has been clarified and the information security framework has been expanded with the addition of new elements.
- A policy methodology has been developed and an information security model has been developed, which is in line with the state and needs of the business environment and the technological environment of Bulgarian organizations implementing electronic commerce.

This monograph is based on a defended dissertation on 02.09.2015 at the Academy of Economics "D.A. Tsenov" - Svishtov at a meeting of the Scientific Jury.

Keywords: information security, e-commerce systems, e-transactions, secure environment, threats, mobile commerce, dimensions, technological solutions, organizational policies, security protocols, industry standards, secure e-payments, policy making methodology -security policy, architectural model of information security solution in e-commerce systems.

Съдържание

ИНФОРМАЦИОННА СИГУРНОСТ КАТО ПРИОРИТЕТ НА СИСТЕМИТЕ ЗА ЕЛЕКТРОННА ТЪРГОВИЯ.....	4
INFORMATION SECURITY AS AN ELECTRONIC COMMERCE	6
SYSTEMS PRIORITY	6
УВОД	10
ПЪРВА ГЛАВА. ИНФОРМАЦИОННА СИГУРНОСТ В СИСТЕМИТЕ ЗА ЕЛЕКТРОННА ТЪРГОВИЯ.....	13
1.1. Информационната сигурност в системите за електронна търговия като изследователски проблем	13
1.1.1. Формулиране на основните постановки и понятийния апарат	13
1.1.2. Проблемът на защитата на информацията и сигурността в електронната търговия	26
1.1.3. Предизвикателства пред сигурността в мобилната електронна търговия	29
1.2. Защитата като нефункционален компонент на системата за електронна търговия	31
1.2.1. Значение на защитата за функциониране на електронната търговия ...	31
1.2.2. Рискът като ключов фактор в информационната сигурност на електронната търговия	32
1.3. Подходи и решения за поддържане на информационната сигурност в системите за електронна търговия	33
1.3.1. Основни аспекти на защитата в електронната търговия	33
1.3.2. Систематизиране на заплахите в електронната търговия.....	36
1.3.3. Тенденции в развитието и заплахите за информационната сигурност на електронната търговия	39
1.3.4. Анализ и управление на риска в електронната търговия	44
ВТОРА ГЛАВА. ТЕХНОЛОГИИ И СТАНДАРТИ, ПОДДЪРЖАЩИ ЗАЩИТЕНА СРЕДА ЗА ФУНКЦИОНИРАНЕ НА ЕЛЕКТРОННАТА ТЪРГОВИЯ.....	52
2.1. Компоненти на защитената среда за електронна търговия	52
2.1.1. Измерения на информационната сигурност в електронните транзакции	53
2.1.2. Технологични решения за информационна сигурност в електронната търговия	54
2.1.3. Организационни политики за управление за информационната сигурност.....	60

2.1.4. Индустриални стандарти и нормативни актове за защита на информацията	61
2.2. Протоколи за сигурност на информацията, използвани в системите за електронна търговия	63
2.2.1. Протоколи за удостоверяване.....	63
2.2.2. Протоколи за сигурност в слоевете на модела OSI.....	65
2.2.3. Протоколи за защита на информацията при различни видове частни мрежи	70
2.3. Сравнителен анализ на стандартите за информационна сигурност, прилагани в електронната търговия	73
2.4. Технологии за реализиране на защитени електронни разплащания.....	80
ТРЕТА ГЛАВА. АНАЛИЗ НА СЪСТОЯНИЕТО И РЕШЕНИЕ ЗА ИНФОРМАЦИОННА СИГУРНОСТ НА ЕЛЕКТРОННАТА ТЪРГОВИЯ В БЪЛГАРСКИТЕ ОРГАНИЗАЦИИ.....	85
3.1. Проблемът със сигурността в българските бизнес организации	85
3.2. Анализ на състоянието на информационната сигурност в системите за електронна търговия на българските бизнес организации	88
3.2.1. Аргументиране на избора и описание на методиката на изследване.....	88
3.2.2. Основни резултати от проучването	90
3.2.3. Изводи от анкетното проучване	114
3.3. Практически мерки за създаване на рамка за информационна сигурност в системите за електронна търговия	115
3.3.1. Формиране на подход към създаване на политика за информационна сигурност.....	115
3.3.2. Елементи на рамката за информационна сигурност в системите за електронна търговия	117
3.3.3. Методология за създаване на политика за сигурност	119
3.3.4. Архитектурен модел на решение за информационна сигурност в системите за електронна търговия	126
ЗАКЛЮЧЕНИЕ	138
ИЗПОЛЗВАНА ЛИТЕРАТУРА	141
СПИСЪК НА ИЗПОЛЗВАНИТЕ СЪКРАЩЕНИЯ.....	149

Увод

Второто десетилетие на XXI век се налага като период на глобално движение на стоки, услуги, капитали и хора. Това е процес, който в своята същност се явява резултат от развитието на информационните и комуникационни технологии и особено в резултат на промените в скоростта, с която се обменя информацията. **Електронната търговия (ЕТ)** е търговия на стоки и услуги посредством глобалната мрежа Интернет или други компютърни мрежи. През последните години оборотите в този тип търговия нараснаха значително и въпреки влиянието на световната икономическа рецесия, се очертава трайна тенденция на ускоряване на този растеж.

Продажбите чрез ЕТ в България отбелязват средногодишен ръст от около 20%, по данни на Националния статистически институт (NSI, 2015). Стойността на реализираните продажби през 2014 г. е 5 млрд. лв. и специалистите прогнозираят този темп да продължи да нараства и в бъдеще. Това се дължи на отсъствието на притеснения при онлайн пазаруване и все по-честото ползване на дебитни и кредитни карти за предварително плащане на стоките – по банков път или чрез електронни системи за разплащане (Георгиев, 2014).

Независимо от отбелязания растеж, проучване на Евростат (Георгиев, 2014) нарежда България на последното място сред страните от Европейския съюз по дял на продажбите, осъществени по електронен път. Въпреки това, изследването показва, че през 2013 г. броят на пазарувалите онлайн е достигнал 683 хил. души, което е ръст от почти 100% спрямо 2011 г., когато те са били около 360 хиляди. Посочените данни представят тенденция на ускорено развитие на ЕТ, а широкото използване на решения за електронни магазини са доказателство за стремежа към ориентиране на дейността на малкия и среден бизнес към виртуалното пространство.

През последните години се наблюдава тенденция на диверсификация на пазара и постоянно появяване на нови електронни магазини. Тенденцията се стимулира и от навлизането на софтуер като услуга (Software as a Service - SAAS) решения за електронни магазини, предоставящи нова, коренно различна бизнес концепция, която минимизира разходите и рисковете при стартиране на ЕТ.

Независимо, че за сега България изостава в развитието на ЕТ, няма съмнения, че този модел на търговия започва да се налага и то много по-бързо от очакванията, тъй като е ефективен за всички страни в търговската транзакция (продавачи, купувачи, платежни системи, логистични фирми и др.). И тъй като ЕТ включва всяка форма на бизнес транзакция, при която страните си взаимодействат по електронен път, а не чрез физически обмен или директен контакт, един от основните ѝ аспекти, който поражда проблеми от техническо, технологично, организационно, психологическо, социално и др. естество е *защитата на предаваните данни* и необходимостта от поддържане на *високо ниво на информационната сигурност*.

Заплахите пред информационната сигурност се увеличиха значително през последните години, като се започне от масовото разпространение на компютърни вируси през 80-те години на XX век, последвано от появата на различни типове вредоносни програми, хакерски атаки и други действия, носещи заплахи за информационната сигурност. Според водещи специалисти (Grant, 2010), работещи в ИТ сигурността, проблемите с информационната сигурност ще продължават и в бъдеще. Като най-атрактивни и съществено уязвими сфери се очертават облачните услуги, мобилните устройства, социалните мрежи и Web 2.0 услугите. Това са и сферите, в които се развива ЕТ.

Поддържането на високо ниво на информационната сигурност е едно от сериозните предизвикателства, пред които се изправят съвременните информационни и комуникационни технологии. За решаването на проблемите в това направление е необходимо организиране на цялостен и задълбочен анализ на всички реални и потенциални заплахи и на тази база - избор и/или разработване на цялостно решение. Характерните черти на съвременните информационни технологии изискват сигурността да се реализира в разпределена среда на интегрирани локални системи. Свързването на системите може да породят значителен брой проблеми с цялостната сигурност на системата, в случай че отделните компоненти не са добре изолирани. Това налага защитата на изолираната среда да се осъществява в контекста на обстоятелството, че от една страна, външните потребители трябва да имат достъп до базите данни на организацията, а от друга страна, локалните системи трябва да предават данни към отдалечени системи, над които нямат контрол. Първият проблем изисква прилагане на локални процедури с широк обхват към външните потребители, с помощта на които се реализира известен контрол върху заплахите към системата и нейния интегритет. Вторият проблем налага мерки за противодействия, които включват имплементиране на нови процедури, които не са част от локалните мерки по сигурността (Емилова, 2006, стр. 189).

Към настоящия момент са проведени редица проучвания за състоянието, технологиите и стратегиите относно информационната сигурност в системите за електронна търговия (СЕТ) от изследователи като Лоудън, Тревър, Крутз, Нахари, Урбачевски, Кинг и др., но в българската теория отсъства обстоен труд, който да е посветен на тази проблематика.

Основната цел на труда е, в съответствие с потребностите на съвременната икономическа теория и практика, да бъде извършено едно сравнително цялостно и систематизирано изследване на проблемите на информационната сигурност в сферата на електронната търговия. Изследването има практико-приложен характер. *Теоретичните проблеми* се изследват с цел анализиране на сложната природа на информационната сигурност и систематизиране на съвременните технологии, средства и методи за постигане на необходимото ниво на сигурност в системите за електронна търговия от тип бизнес към клиент (Business to customer - B2C). *Приложната цел* включва разработване на методология за изграждане на рамка за информационна сигурност, очертаваща стратегия, политика и архитектурен модел, които да могат да се приложат от функциониращите в тази сфера български бизнес организации.

Така дефинираната цел се постига с решаване на следните **изследователски задачи**:

- изясняване на същността на *понятията информационна сигурност и защита* като основни компоненти на системите за електронна търговия;
- осъществяване на критичен анализ на съвременните *информационни и комуникационни технологии, подходи, решения и стандарти*, поддържащи защитена среда за функциониране на електронната търговия от тип бизнес към клиент;
- организиране и провеждане на *анкета* с участието на специалисти от практиката за установяване на текущото състояние на информационната сигурност в бизнес към клиент системите за електронна търговия на бизнес организациите в България;
- анализиране на *състоянието на информационната сигурност* в системите за електронна търговия от тип бизнес към клиент в български организации на база проведената анкета;
- изясняване на *подход за създаване на политика* за информационна сигурност и разширяване на рамката за информационна сигурност с нови елементи;

- разработване на *методология за политика и изграждане на модел* за информационна сигурност, който да е в съответствие със състоянието и потребностите на бизнес средата и технологичното обкръжение на български организации, осъществяващи електронна търговия;

Изследователската теза в разработката е, че информационната сигурност е новен и жизненоважен приоритет за ефективното функциониране на системата за електронна търговия. Тя има сложна и многопластова природа. За да е резултатна, информационната сигурност трябва да съчетава адекватни на бизнес средата технологии, закони, политики, процедури и индустриални стандарти.

Обект на изследване в настоящия труд са системите за електронна търговия от тип бизнес към клиент (Business to customer - B2C) в българските компании.

Предмет на изследване е информационната сигурност на тези системи, постигана чрез съвкупност от различни подходи, стратегии, методи, политики, техники и технологии.

За **методологическа база** на изследването се използва системният подход. Приложени са и други подходи и методи като сравнителен анализ, индуктивен и дедуктивен методи, метода на моделирането и др.

Емпиричното изследване се осъществява чрез практическо проучване посредством анкетна карта и събеседване с ръководните органи на водещи организации, осъществяващи електронна търговия. В хода на изследването бяха селектирани 171 електронни магазина, на които са изпратени анкетни карти. Направените изводи и анализи се базират на отговорите на 36 респондента. Използваната методология включва експертно анкетно проучване чрез анкетна карта, съдържаща 32 въпроса за установяване състоянието на информационната сигурност в системите за електронна търговия на изследваните организации.

Резултатите са анализирани със специализирания софтуерен продукт SPSS на IBM.

Първа глава. Информационна сигурност в системите за електронна търговия

1.1. Информационната сигурност в системите за електронна търговия като изследователски проблем

За решаване на задачите, които си поставяме с настоящето изследване, е необходимо да бъдат дефинирани и конкретизирани няколко основни понятия, като електронен бизнес (ЕБ), електронна търговия (ЕТ), дигитални стоки, информационна безопасност, информационен риск. Това са понятия, които в научната литература авторите интерпретират от различни гледни точки, с различни цели и по тази причина - с различна степен на обобщеност.

1.1.1. Формулиране на основните постановки и понятийния апарат

Първоначално електронната търговия се свързва с осъществяване на търговските сделки по електронен път чрез използване на технологии като електронен обмен на данни (ЕОД) и електронен превод на средства (ЕПС). Въведени в края на 1970 г. (Basaga, 2013), те допринасят за развитие на бизнеса посредством изпращане на търговски документи, като заявки за покупка или фактури по електронен път.

Към настоящия момент се приема, че ЕТ е съвършено нов подход за осъществяване на бизнес сделки. Изясняването на същността ѝ налага нейното разглеждане от различни аспекти и въвеждането на споменатите по-горе понятия - електронен бизнес, разликата между ЕТ и ЕБ, дигитални стоки и др.

1) Електронен бизнес

Електронният бизнес е понятие, възникнало в процеса на масовизиране на използването на Интернет за целите на бизнеса. За първи път терминът се въвежда през 1997 г. от IBM, когато компанията осъществява кампания за популяризиране на ЕБ и разширяване на подходите към бизнес дейностите, извършвани чрез мрежата. Първоначално е имало две основни становища за ЕБ. Първото (Benjamin, 1993) ограничава ЕБ до ЕТ, а второто (Zwass, 1996) включва в понятието ЕБ всички бизнес дейности на организацията, извършвани посредством мрежово ориентирани компютърни технологии. Последвалото развитие на ЕБ обаче доказва, че това е един многоаспектен феномен, който трябва да се разглежда от различни аспекти.

В изследването на ЕБ авторите прилагат различни подходи, каквито са икономически, технологичен, системен, стратегически, процесен подход и др. Така например, съчетавайки технологичен и стратегически подход, Амор (Амор, 2000) определя ЕБ като оползотворяване на удобството, наличността и достъпността до всички световни ресурси, за да се развие реалния бизнес или да се формира нов виртуален бизнес.

Подобно е и схващането на Върбанов (Върбанов, 2004), който дефинира ЕБ като всяка форма на използване на съвременните ИКТ в бизнеса, като по този начин се добавя нова стойност към продукта, който се създава и се въвеждат нови и ефективни методи за правене на бизнес в Интернет.

Автори като Шишманов (Шишманов, 2004) прилагат основно системния подход и разглеждат ЕБ като система за осъществяване на бизнес дейности, основаваща се на използването на съвременни ИТ при организацията на контактите между участниците в сделките.

Процесен подход прилагат при дефинирането на ЕБ и специалистите от IBM, за които ЕБ представлява промяна на същността на ключовите бизнес процеси чрез използването на Интернет технологии (Schneider, 2012).

Един комплексен подход, съчетаващ процесен, системен, стратегически и технологичен подходи откриваме в определението на Емилова (Емилова П. , 2002), според която ЕБ е осъществяване на бизнес процеси в организацията (външно- и вътрешно-ориентирани), поддържане на бизнес отношения и съвместно използване на бизнес информация, на основата на съвременните ИТ, с цел повишаване на ефективността и постигане на стратегическите цели на компанията. Освен всичко друго, в това определение се откроява и обектът на ЕБ, а именно – бизнес процесите, бизнес отношенията и бизнес информацията на организацията. Това определение изразява най-пълно същността на електронния бизнес и дава цялостна визия за обхвата му.

2) Електронна търговия

Следващото основно понятие, което е наложително да уточним и е пряко свързано с обекта на настоящия труд, е електронна търговия.

Важно е да се прави разлика между понятията ЕБ и ЕТ. ЕТ засяга основно процесите, свързани с външни партньори като доставчици, клиенти, както и дейностите по реализирането на стоките, включващи маркетинг, приемане на поръчки, реклама и други. ЕБ включва ЕТ, както и други бизнес дейности като производство, мениджмънт, финанси и др. Различията между ЕБ и ЕТ са дефинирани от различни автори, например Еймор. Според него “електронният бизнес има за цел да използва преимуществата на Интернет, както за разширяване възможностите на традиционния бизнес, така и за създаване на нови, виртуални видове бизнес”, а “електронната търговия е само едно от направленията на електронния бизнес, както електронния франчайзинг или електронния маркетинг“ (Еймор, 2001).

В документите на Европейския съюз, ЕТ е дефинирана като „всяка форма на бизнес сделка, в която страните взаимодействат електронно“.

Според Лоудън и Тревър (Laudon K. T., 2013), ЕТ е цифрово активирана търговска сделка (комерсиална транзакция), която се осъществява между и сред организации и индивиди. Като търговска сделка, ЕТ задължително предполага размяна на стойност (пари) през организационни и/или индивидуални граници в замяна на продукти или услуги. Размяната на стойност е важна за разбирането на границите на ЕТ. Без размяна на стойност не се осъществява търговски прогрес. Затова авторите смятат, че ЕБ се отнася предимно за цифрово реализиране на транзакции и процеси вътре в организацията, включвайки информационните системи, контролирани от нея. В основната си част ЕБ не обхваща търговски сделки през организационните граници, където се разменя стойност.

Едно от най-разпространените схващания е, че ЕТ е форма на бизнес отношения, при които взаимодействието между индивидите се осъществява по електронен път (Краева, 2009) . Това се свързва с поставянето на дадена стока или услуга в уеб пространството, което продължава с осъществяване на разплащания по определен механизъм и т.н.

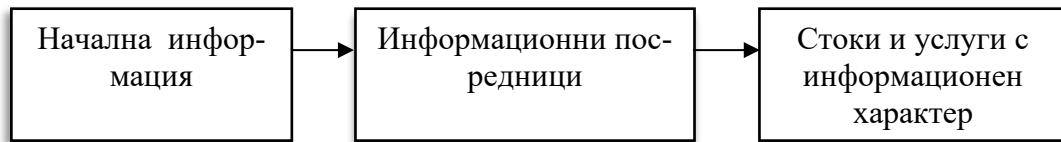
Друга възможност за по-задълбочено разкриване на същността на ЕТ, е на база създаването на така наречената **цифрова стойност**. Формирането ѝ се възприема като иновативен производствен процес, който е основният елемент в ЕТ. Създаването на цифрова стойност според нас, може да се разгледа като процес на трансформиране на началната цифрова информация за стойността в крайна такава с добавена стойност. Тази трансформация обхваща два момента:

- процес, при който информацията се използва като ресурс;

- от този ресурс чрез обработка се получават стоки и услуги с информационен характер и с добавена стойност.

Така разгледана, ЕТ се възприема като процес, който се извършва изцяло по електронен път.

Процесът на създаване на цифровата стойност е представен на фиг. 1.1.



Фиг. 1.1. Процес на създаване на цифрова стойност

Главната цел на информационните посредници в разглеждания процес е да формират нова цифрова стойност, като посредническите организации взаимодействат с източниците на информация и генерират крайния продукт под формата на дигитален продукт или друга форма на обработена информация. Посредниците извършват дейност в една новедефинирана стойностна верига, за която реално не съществуват граници. Това допринася за разпространението на т.нар. дигитални цифрови пазари.

Обобщено, разглеждането на ЕТ на база на описаната концепция поддържа твърдението, че този вид търговия се отнася за организации и потребители, които усвояват новите похвати и методи на провеждане на бизнеса помежду си. Тези похвати и методи се поддържат чрез електронните отношения и взаимодействия, които елиминират изискванията за физическо посещение на обектите при осъществяването на търговията.

ЕТ е дефинирана също и в нормативни документи като Закон за електронната търговия и др.

Обобщавайки различните становища за ЕТ можем да изведем следната дефиниция – ЕТ включва всички покупки-продажби, извършвани по електронен път чрез глобалната мрежа Интернет или друга компютърна или комуникационна мрежа. Тя представлява комплекс от технологии и бизнес процеси, който включва електронен обмен на данни, електронни транзакции, превод на финансови средства, управление на системи за доставка, електронен маркетинг и др.

Характерно за ЕТ е, че в зависимост от страните, между които се осъществяват транзакциите, тя се реализира чрез множество модели, двата най-разпространени от които са бизнес към клиент – **B2C** и бизнес към бизнес – **B2B**.

Моделът B2B е с най-голям дял по стойност на извършените транзакции и обхваща взаимоотношенията между различни компании, като информацията се обменя през частни мрежи и мрежи с добавена стойност.

B2C е модел, при който купувачът (индивидуалният краен клиент) плаща директно на търговеца за дадена стока или услуга (Radu, 2003) и е с най-голям брой извършени транзакции. Той е сравним с търговията на дребно и може да се осъществи чрез различни типове електронни магазини, които предлагат потребителски стоки от разнородни категории.

Изследването в настоящата разработка е насочено към модела B2C. Този модел се отличава с по-големия брой извършвани транзакции от различно естество и непрекъснатите заплахи за сигурността. Сред най-съществените **предимства на B2C са** (Main advantages (B2C)): диференциран подход към индивидуалността на всеки клиент; по-малка ангажираност на капитала и намаляване на свръхпроизводството; по-добро познание на потребителските нужди; по-висока потребителска лоялност; широк асортимент от стоки; пазаруване като опит.

При проучването на ЕТ от тип В2С се вижда, че тя се осъществява чрез така наречените **виртуални магазини** (Newman, 2002)- магазини, при които продавачът общува с клиентите посредством компютърна програма или други комуникационни устройства. Понятието *виртуален* се дефинира като възможен, вторичен, който може или е задължително да се прояви при определени обстоятелства. В този смисъл ЕТ представлява осъществяване на покупко-продажби чрез глобалната мрежа, а виртуалният магазин се отъждествява с уеб сайт, чрез който е възможно интерактивно закупуване или продаване на стоки или услуги. За нормалното функциониране на един виртуален магазин трябва да се спазват задължителни препоръки, които са част от политиката за сигурност на организацията. Те са описани подробно в глава 3, т. 3.3 на настоящия труд.

Задължителните взаимосвързани елементи в организацията на електронния магазин, дефинирани от Шишманов (Шишманов, 2004), са: електронна витрина; система за поръчки; връзка към система за разплащане; връзка към система за доставка.

Обектите на покупко-продажба в електронните магазини са от най-различно естество и могат да бъдат класифицирани в следните групи:

- **материални стоки** – стоки за бита като книги, напитки, електроника и др.;
- **нематериални стоки** – това е информацията, която се доставя чрез глобалната мрежа. Тази информация може да бъде под различна форма – новини, каталози, видео, страници, софтуер и т.н.;
- **виртуални интерактивни услуги** – основават се на нови и съществуващи услуги. Тук се включват резервации, наемане на коли под наем, различни туристически услуги, банкови услуги, финансови услуги и т.н.;
- **символични стоки с цифрова стойност** – представляват информационни стоки, продукти, които предоставят на потребителите определени права за достъп до други стоки и услуги на физическия пазар. Такива са смарт картите, електронните пари, електронните портфейли и някои други.

Чрез електронните магазини се осигурява покупко-продажба на разнообразни стоки и услуги. В глобалната мрежа Интернет присъствието на електронния магазин най-често се осъществява от доставчик на услуги за уеб хостинг (С., 2005). Освен това, той осигурява услуги за съхранение, Интернет свързаност и поддържа уеб сайтове, на принципа на абонамента.

3) Електронни разплащателни системи

Освен електронните магазини, за ЕТ важно значение имат и **електронните разплащателни системи**. Те използват цифрови технологии за трансфер на електронни пари, извършване на транзакции чрез кредитни карти, смарт карти и дебитни карти. Основен приоритет за всяка организация е да е запозната с предимствата и проблемите при електронните разплащания, поради ежедневната им приложимост.

В по-голямата си част съществуващите механизми за плащане могат да бъдат адаптирани към онлайн средата, дори и със значителни ограничения, които са довели до развитие на алтернативи. Освен това появата на нови видове търговски взаимоотношения (като онлайн търговия между индивиди Peer to Peer- P2P) и нови технологии (като развитието на мобилните платформи) създадоха, както необходимостта, така и възможността за развитието на нови платежни системи.

Основните тенденции в развитието на ЕТ разплащания за 2012 – 2013 г. са очертани от Лоудън и Тревър (Laudon K. T., 2013):

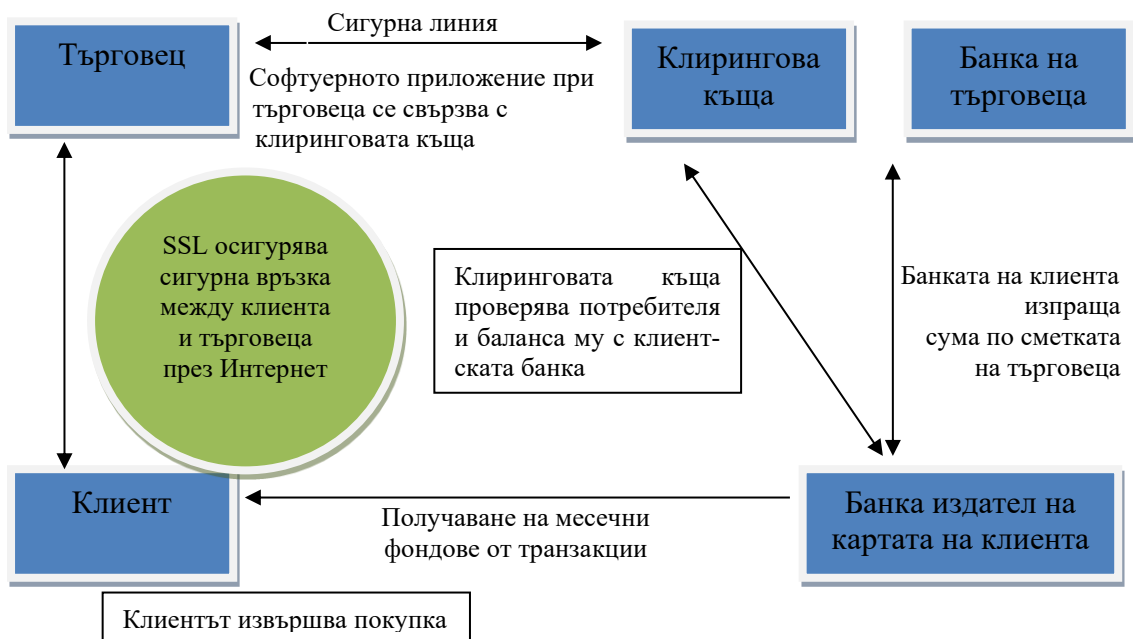
- плащането с кредитни и/или дебитни карти остава доминираща форма на онлайн разплащанията;
- най-популярната алтернатива на онлайн методите за разплащане остава PayPal;

- започва да се утвърждава Start-up Square¹ чрез приложенията за смартфони, четци за кредитни карти, както и услуги за обработване на кредитни карти, които позволяват на всеки потребител да приема плащане с кредитна карта;
- мобилна система за плащане Google Wallet, базирана на Near Field Communication (NFC) чипове.

Онлайн транзакции с кредитни и дебитни карти

Тъй като кредитните и дебитните карти са доминираща форма на онлайн плащания е важно да се разбере начинът на функционирането им и да се оценят предимствата и недостатъците им.

Онлайн транзакциите с банкови карти се обработват аналогично на покупка в магазин, с основна разлика, че продавачът не вижда използваната карта и не получава потвърждение за транзакцията чрез саморъчния подпис на купувача.



Фиг. 1.2. Цикъл на онлайн плащане с банкови карти, източник (Laudon К. Т., 2013)

Цикълът на онлайн плащане с банкови карти е представен на фиг. 1.2., където са включени пет типа потребители, които участват в покупката, заплащана с банкова карта: клиент; търговец; клирингова къща; банка, обслужваща търговеца (понякога наричана акцептираща/придобиваща банка); банка, обслужваща картата на клиента. За да се предприеме онлайн плащане чрез банкова карта, е необходимо потребителите да имат сметка в банка или финансова институция, която позволява на компаниите да обработват плащания с банкови карти и да получават фондове от тези транзакции, наречена **търговската сметка (merchant account)**. Компаниите, които имат търговска сметка, трябва да осигурят и средства за управление и защита на онлайн транзакцията. В това направление множество компании–доставчици на услугата за разплащане през Интернет могат да доставят както търговска сметка, така и софтуерни инструменти, необходими за обработване на онлайн покупката чрез кредитна карта. Такава компания е световноизвестният доставчик на услуги CyberSource.

¹ Start-up Square е компания за мобилни плащания, която позволява на магазините да приемат кредитни/дебитни карти през телефони и таблети и дейността ѝ включва онлайн фактуриране и депозити.

Съществуват множество **ограничения на системата за онлайн разплащания** с банкови карти. Най-съществените от тях са свързани със сигурността, риск за търговеца, административни и транзакционни разходи и социална справедливост.

Първият основен проблем се свежда до това, че съществуващите системи предлагат слаба защита. При тях нито клиентът, нито търговецът могат да получат пълна автентификация. Търговецът може да бъде криминална организация, чиято цел е да събира информация за кредитни карти, а клиентът може да е злонамерено лице, използващо чужда (крадена) кредитна карта. Рискът за търговеца е по-голям: клиентът може да откаже плащането, дори продуктът да е изпратен или изтеглен. Поради тези проблеми банковата индустрия прави опити да развие протоколи за защитени електронни транзакции като Secure electronic transaction (SET), но тези усилия пропадат, защото това е еднакво сложно и за клиентите и за търговците.

На второ място, административните разходи за създаването на една онлайн система за разплащане с кредитни и дебитни карти и авторизирането ѝ за приемане на тези карти са високи. Транзакционните разходи за търговците също са значителни – приблизително 3.5% от покупката плюс транзакционната такса от 20-30 цента за транзакция, плюс други такси.

И на последно място, кредитните и дебитните карти по своята същност не са много достъпни, въпреки че създават впечатлението, че са повсеместно разпространени, факт е, че милиони хора не ползват такива карти.

В България потребителският интерес към картовите разплащания непрекъснато нараства. Ежегодното проучване MasterIndex на MasterCard показва, че дебитните и кредитните карти неизменно присъстват в ежедневието на българските потребители и че те редовно използват банкови карти, дори и за всекидневни рутинни плащания, като предимно се използват дебитни карти (Econ.bg, н.д.).

Електронните разплащания с дебитни и кредитни карти в България отчитат значителен ръст през 2013 г., показва изследване на технологичната компания Visa Европа (Darkfinance.bg, n.d.). Според проучването, размерът на плащанията с карти Visa, издадени от български финансови институции, отбелязва растеж от 27% годишно и превишава 1,148 млрд. евро. Електронните разплащания с карти Visa, обслужвани от български банки, достигат 167 млн. евро, което е приблизително 92% ръст през 2013 г. Тези показатели можем да обясним с масовото навлизане на електронните разплащания сред българските потребители и онлайн търговци.

Разглеждайки значението на банковите карти в разплащателния процес, е необходимо да се посочи, че те се използват не само за теглене на пари в брой от банкомати или ползване на ПОС терминали, но са и основен платежен инструмент в много от приложенията в Интернет (Бойчев, Шишманов, & Маринова, 2016, стр. 44). Въпреки това ограниченията на онлайн системата за разплащане с дебитни и кредитни карти откриват път за развитието на множество **алтернативни онлайн системи за разплащане**. Водеща сред тях е PayPal, придобита от eBay през 2002 г. Системата PayPal позволява на индивидуалните потребители и бизнеса, които имат имейл акаунт, да извършват и получават плащания до определени граници. Тя е пример за онлайн система за плащане, базирана на съхранена стойност, която позволява на потребителя да извършва незабавни онлайн плащания към търговци и други индивиди на база стойност, съхранена в онлайн сметка. **Предимството** на PayPal е, че между потребителите не трябва да се споделят лични данни за техните банкови сметки. Също така, услугата може да бъде използвана с цел отделните индивиди да извършват плащане помежду си. **Проблемите** при използването на PayPal са свързани с високите разходи (в допълнение на плащането на таксата по кредитната карта, PayPal добавя такса от 1.5% до 3% в

зависимост от размера на транзакцията) и липсата на защита на потребителите в случай на извършване на измама или на отказ от извършване на плащането.

Въпреки, че PayPal е най-популярната онлайн система за плащане съществуват и други **алтернативи** за електронни разплащания. Популярни към момента са (Baker, 2015):

- **Amazon Payments** е ориентирана към потребителите, които избягват да предоставят личната информация за кредитната си карта на непознати онлайн търговци;
- **Google Checkout** – система, обединена с Google Wallet и предлага подобна функционалност, давайки възможност на потребителя да се регистрира веднъж и след това да пазарува онлайн от хиляди различни магазини, без да трябва отново да въвежда лична информация за сметката си;
- **Bill Me Later** осигурява функционалността на предходните две системи;
- **WUPay** – система, позната като eBillme, която към настоящия момент оперира с Western Union и предлага подобна услуга;
- **Dwolla** е кеш-базирана мрежа за разплащане, използвана от клиенти и от търговци, която заобикаля мрежата на кредитните карти и вместо това се свързва директно с банковата сметка;
- **Strip** е компания, подобна на Dwolla, която предлага алтернатива на традиционната онлайн система за плащане с кредитни карти. Тя се фокусира върху страната на търговеца и осигурява прост софтуерен код, който позволява на компаниите да прескочат повече от административните разходи, включени в създаването на една онлайн система, използваща кредитни карти.

Българските разплащателни системи също набират популярност през последните години. Основните от тях са (PayZone, n.d.):

- **ePay.bg** е доставчик на платежни услуги в България, който е сертифициран от VISA и MasterCard и присъства в списъка от доставчици, публикуван на техните сайтове;
- **eBG.bg** е технологична система, която е разработена при високи гаранции за сигурност и надеждност от високо квалифицирани и опитни специалисти в сферата на прилагането на нови технологии. От края на 2013 г. системата не функционира;
- **RINGS (Real-Time Interbank Gross Settlement System)** е платежна система, изградена от Българската народна банка, чиято цел е прехвърляне на парични средства между сетълмент-сметките на участниците в нея окончателно, индивидуално и в реално време след получаване от системата на нареждането за превод (BNB, n.d.);
- **Easypay** е система, която осигурява възможност на клиентите да извършват плащания и парични преводи от удобен офис, без значение от местоположението им, като спестява време и средства, гарантира сигурността и надеждността за всички видове плащания;
- **Плащане чрез SMS от мобилен телефон** позволява да се заплати за избраната услуга, без значение от времето и мястото;

Мобилни системи за разплащане

Използването на мобилните устройства като механизми за плащане вече е добре установено в Европа, Япония и Южна Корея и бързо нараства в САЩ. **Near Field Communication (NFC)** - комуникация от близки разстояния е комплекс безжични технологии с малък обем, използвани за споделяне на информация между устройства (Androidbg, n.d.). Устройствата с вграден NFC чип могат да приемат и предават данни на друго устройство от този тип на разстояние 4-10 см. Функционирането на малки разстояния намалява вероятността от интерференция и превръща NFC в подходяща технология за места, където се осъществяват бързо разплащания. Връзката между

устройствата се установява за части от секундата, като не е нужно да се правят допълнителни действия или настройки преди насочване към използване на NFC карта, телефон или друго устройство, поддържащо технологията. Това намалява значително възможността информацията да бъде прихваната, докато се плаща.

Посредством NFC, персоналният мобилен телефон се превръща във виртуален портфейл. Технологията притежава потенциал мобилните устройства да изместят банковите карти. NFC намира приложение и в транспорта – закупуване на всякакъв тип билети чрез мобилни устройство и др.

През септември 2011 г. Google представи Google Wallet, мобилно приложение, проектирано да работи с NFC чипове. Към настоящия момент Google Wallet работи с MasterCard PayPal – система за плащане, използваща безконтактни карти. Те са проектирани да работят и с Android смартфони, които са оборудвани с NFC чипове. PayPal и стартиращият Squire атакуват пазара за мобилни плащания от по-различна позиция - с приложения и четци за кредитни карти, които се прикрепят към смартфоните.

Дигитални пари и виртуални валути

Въпреки, че термините дигитални пари и виртуална валута често се използват като синоними, в действителност те се отнасят до два отделни типа алтернативни системи за плащане. **Цифровите пари** се базират на алгоритъм, който генерира уникални, автентифицирани символи, представящи парична стойност, която може да бъде използвана в реалния свят. Основните им характеристики се свеждат до независимост, сигурност, анонимност, плащане офлайн, прехвърлимост и делимост.

През януари 2009 година беше създадена **Bitcoin**, която представлява нов вид виртуална валута. Първоначално тя се използва само от любителите на виртуалната, компютърна реалност, но по-късно тя се превръща в популярен начин за разплащане сред потребителите в реалния свят, а също и в инвестиционен инструмент. Повишеното внимание към Bitcoin дава отражение върху стойността му - четири години по-рано, при пускането на виртуалната валута, курсът ѝ бе един Bitcoin за 5 цента, а към края на 2013 г. - 98,25 долара (Биткойн, 2013).

Виртуалната валута обикновено циркулира в едно виртуално интернет общество или е издадена от определена корпоративна единица и се използва за закупуване на виртуални стоки, като Linden Dollars, създадени от Linden Lab за използване в нейния виртуален свят Second Life, или свързани със специфична корпорация като Facebook Credits. И двата типа най-често се използват за закупуване на виртуални стоки.

Електронно фактуриране и плащане

По мнение на експерти разходите за реализиране на жизнения цикъл на една хартиено базирана фактура в бизнеса, стартиращ от точката на издаване и достигащ до точката на плащане, варират между 3 и 7 долара (Fiserveys, 2007). Тази калкулация не включва стойността на времето, необходимо за отваряне на фактурата, прочитането ѝ, написването на чек, адресирането на пощенски плик и изпращането на чека по пощата. Този процес по изпращане и плащане на фактури предоставя една изключителна възможност за използване на Интернет като електронна система за изпращане и плащане на фактури/сметки, която може съществено да намали, както разходите за плащане, така и времето, което клиентите изразходват за това плащане. Изчисленията варират, но се счита, че средните разходи по едно онлайн плащане са в диапазона 20 – 30 цента.

Системите за електронно фактуриране и плащане - Electronic bill presentment and payment (EBPP) осигуряват възможност за онлайн доставка и плащане на месечни сметки. EBPP-услугата позволява на клиента да провери електронните сметки и да ги плати чрез трансфериране на електронни фондове от банкови сметки или кредитни карти.

Бизнес модели за електронно фактуриране и плащане ЕВРР

В сферата на електронно фактуриране и плащане (ЕВРР) съществуват два конкуриращи се модела: директно плащане (biller-direct) и консолидатор (consolidator).

Системата за **директно плащане** първоначално е създадена за удобство на компаниите, които ежесечно изпращат милиони сметки. Целта ѝ е да улесни клиентите при техните рутинни онлайн плащания. Компаниите, прилагащи директно плащане могат също така да развият собствена вътрешна система, инсталирайки система, придобита от трета страна - доставчик на ЕВРР софтуер; използвайки ЕВРР, като услуга от трета страна или използвайки доставчик на приложения.

При **консолидиращия модел**, трета страна, която може да бъде финансова институция или портал, събира всички сметки за потребителите и осигурява плащане на сметките. Практиката показва, че финансовите институции са по-търсени от порталите при онлайн плащането на потребителските сметки. Въпреки това, консолидаторите са изправени пред множество предизвикателства:

- за бизнеса - използването на модела на консолидиране означава увеличаване на времето между издаването на сметката и плащането, както и вмъкване на посредник между компанията и нейните клиенти;
- за клиентите основен проблем е сигурността - повечето клиенти не са склонни да споделят личните си финансови данни с нефинансови институции, а също и да плащат такса за това, че плащат сметките си онлайн.

4) Дигитални стоки

Това са стоки, които се произвеждат, съхраняват и доставят в електронен формат (Bauknecht, 2003). При закупуване на такива стоки, след осъществяване на заплащане, на клиента се предоставя приложение, осигуряващо сигурна връзка за електронна поща или линк към сървър за получаване на дигиталната стока.

5) Електронната търговия като обект за изследване

Електронната търговия представлява технологичен, икономически и социален феномен, който изисква извършване на бъдещи проучвания в три основни направления – технологии, бизнес и общество.

Съвременните възгледи за изследване на ЕТ са се формирали като резултат от динамичното ѝ развитие. В множество публикации в специализираната литература се наблюдава изместване на фокуса на изследванията за ЕТ. Така например Суун Юнг Чои, Андрю Уинстън и Дейл Стал представят основните аспекти на ЕТ в „Икономиката на Електронната Търговия“ - техническо изследване, икономическо изследване, въпроси по продуктите и бизнес процеси (Choi, Whinston, & Stahl, 1997).

Според Урбачевски и други направленията за изследване на ЕТ се класифицират в 4 категории: организационни, икономически, технически и други (Urbaczewski, 2002).

Нгай и Уат също определят 4 категории на изследователската литература, насочена към ЕТ: приложения, технологични проблеми, поддръжка и изпълнение (Ngai, 2002).

Кауфман и Уолдън представят изследване на ЕТ, насочено към икономическия анализ. Те предлагат ръководство за изследване на всяка определяна от тях категория и дефинират свързана информационна технология и икономическа теория (Kauffman, 2002). Направленията, към които фокусират вниманието си авторите, включват: технологични проблеми, въпроси по продуктите, бизнес процеси, пазарни проблеми и макроикономически проблеми.

Автори като Стефано Корпер и Хуанита Елис в книгата „Електронна търговия“ изследват детайлно ЕТ, основно в технологичен и бизнес аспект (Corper, 2001).

Дейвид Кинг и други дефинират следните насоки за изследване: електронни пазари, продажби в ЕТ, иновативни системи в ЕТ, динамична търговия (King, 2009).

Ефрейм Турбан и Дейвид Кинг изследват множество нови аспекти на ЕТ, включващи мениджърски и технологични. Авторите представят нови теми като социална търговия, глобална перспектива и др. (Turban, 2012).

Лоудън и Тревър изследват ЕТ в три основни аспекта: бизнес, технология и общество (Laudon K. T., 2013). Те очертават перспективите на всеки от аспектите и развиват нови насоки за изследване – мобилна, дигитална интернет платформа, социални мрежи, онлайн изолiranост и сигурност в Интернет.

При изследване на ЕТ основно се използват два основни подхода: технологичен и поведенчески.

При технологичния подход ЕТ е обект на изследване от компютърните науки, мениджмънта, както и мениджмънта на системите и макроикономиката.

От поведенческа гледна точка, ЕТ се изследва от маркетинга, социологията, мениджмънта, финансите и счетоводството.

Основните тенденции за изследване в областта на ЕТ се фокусират в три аспекта: технология, бизнес и общество (Laudon K. T., 2013).

Технологията има отношение към мобилните платформи, които продължават сериозно да се конкурират с настолните компютри; облачните технологии, осигуряващи достъп до ресурси в интернет пространството чрез клиентско устройство; масовите данни (*Big data*) и разнообразния аналитичен софтуер.

б) Информационна сигурност

Понятието информационна сигурност има широк обхват и включва защитата на информацията и информационните системи от неоторизиран достъп, използване, разкриване, промяна, прочитане, запис и унищожаване.

Понятията *информационна сигурност*, *компютърна сигурност* и *защита на информацията* нерядко и погрешно се употребяват като синоними (Информационна сигурност, n.d.). Тези понятия са свързани и имат общи приоритети като конфиденциалност, интегритет и достъпност на информацията, но съществува разлика между тях, която ще направим опит да изясним.

Информационната сигурност представлява защита на информацията, без значение от формата ѝ – дигитална, върху материален носител и други.

Компютърната сигурност е насочена към изправното функциониране на компютърните системи и мрежи и обработваните от тях данни.

Информационна защита има отношение към техниките по управление на рисковете, които се отнасят до потреблението, съхраняването и придвижването на информацията, както и на оборудването, използвано за тези цели.

В транзакциите, реализиращи ЕТ, циркулира огромно количество чувствителна информация, която включва информация за служители, клиенти, продукти, нови разработки, финанси, банкови сметки, пароли и др. Значителна част от тази информация, а за някои организации и цялата, се събира, обработва и съхранява в електронен вид. Поради това, компютърната сигурност, информационната защита и циркулиращата информация са главната цел на информационната сигурност.

Някои автори разглеждат информационната сигурност в по-тесен смисъл и я дефинират като защита на информацията от широк спектър заплахи с цел осигуряване на непрекъсваемостта на бизнеса, минимизиране на бизнес рисковете и максимизиране на възвръщаемостта от инвестициите и бизнес начинанията (Hintzbergen, 2010).

Автори като Семерджиев, разглеждат информационната сигурност в по-широк смисъл (Семерджиев, 2007). Той я определя като „защитеност на системите на стратегическо, оперативно и тактическо равнище от всякакви опити за“:

- нарушаване на неприкосновеността, достоверността, конфиденциалността, селективността и отказоустойчивостта на достъпа до информационните ресурси;
- несанкционирано ползване, манипулиране или разрушаване на информационните ресурси;
- отслабване или премахване на възможностите за създаване, събиране, разпространение, обработка, съхранение и ползване на информацията;
- несанкционирано ползване, манипулиране или разрушаване на информационната инфраструктура;
- манипулиране на създадените правила и процедури, регулиращи отношенията във връзка с информацията;
- целенасочено дезинформиране на служители, потребители или мениджмънта.

Ние приемаме дефиницията на Семерджиев, тъй като тя обхваща подробно всички аспекти на информационните системи и проблемите на сигурността в тях.

Модел на информационната сигурност

Най-популярният модел на информационна сигурност има три основни аспекти – конфиденциалност, интегритет и достъпност (вж. фиг.1.3). В научната литература се срещат и други модели (Whitman, 2010), които разширяват представеният на фиг. 1.3.

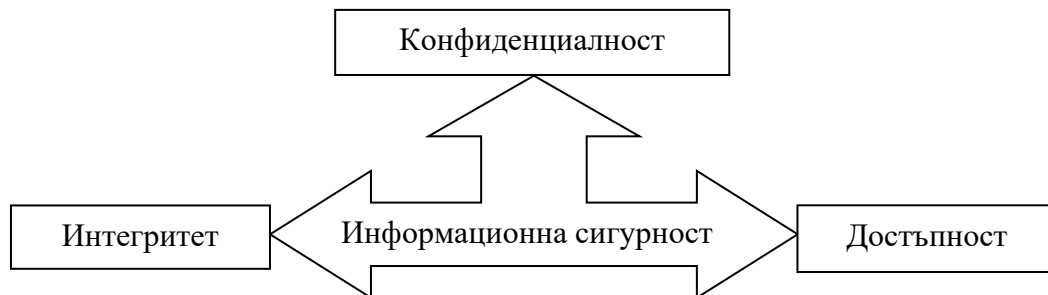
Конфиденциалността се свързва с предотвратяване разкриването на важна информация като лични данни, данни за кредитни карти и клиентски номера от неототоризирани лица или системи (Confidentiality, Integrity & Availability, n.d.). Гарантирането на конфиденциалност на информацията налага съобразяването с определени правила и избягването на рискови действия с чувствителна информация. Такова рисково действие може да бъде например предаване на некриптирани данни през компютърна или телефонна мрежа, когато няма физически контрол върху преносната среда. Рискова среда могат да бъдат телефонни мрежи, Интернет, виртуални частни мрежи без механизми на криптиране. Заплахите за конфиденциалността на информацията са възможни и на вътрешно фирмено ниво, когато например небрежен служител остави на екрана чувствителна информация; кражба или загуба на мобилен компютър или флаш памет.

Интегритетът е характеристика на информационната сигурност, която се отнася до надеждността, произхода, пълнотата и точността на информацията, както и предотвратяване на злоупотреба или неразрешено модифициране на информацията. Интегритетът има отношение не само към целостта на самата информация, но и към интегритетът на произхода на информацията (интегритет на източника на информация).

Интегритетът на информацията се нарушава вследствие на умишлено или несъзнателно унищожаване на важна информация, в резултат на зловреден софтуер, инсталиран в компютъра, когато служител или външно лице добие възможността неототоризирано да модифицира информация. Механизмите за защита на интегритета могат да бъдат групирани в две основни групи: превантивни механизми като контрол на достъпа (които предотвратяват неототоризирана промяна на информацията), както и механизми за разследване (предназначени за откриване на неототоризирани модификации), когато превантивните механизми са се оказали неуспешни. Контролните действия, които защитават интегритета включват принципите на най-малка привилегия, разделяне и ротация на задълженията.

Достъпността се свързва с възможността информацията да бъде винаги на разположение (да е налична), когато е необходима, както и за системите, обработващи и съхраняващи информацията, мерките за безопасност и каналите за комуникация, използвани за предаването ѝ, да работят коректно. Достъпността има и отношение към това техническата и програмната част на компютърната система да функционират ефективно и системата да разполага с опция за бързо възстановяване, в случай на бедствие.

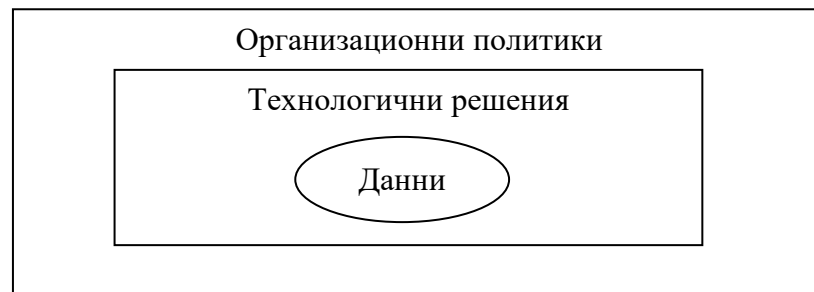
В конкретна среда един аспект на сигурността може да бъде по-важен от другите. При проектирането за всички отделни информационни ресурси е необходимо да се направи преценка на изискванията за вида сигурност, която ще оказва влияние върху избора на специфичните технически средства и продукти за удовлетворяването на тези изисквания. Често, в отвореното информационно общество, достъпността е основно изискване. В случай, че няма достъп, ако не може да се използва компютърната система, няма възможност да се разбере дали конфиденциалността и интегритетът постигат целта си. Дори потребители, за които сигурността не е приоритет, се съгласяват, че компютърните им системи трябва да поддържат работата си.



Фиг. 1.3. Модел на информационна сигурност, източник: адаптирано по (Infosecinstitute, n.d.)

Мерки за осигуряване на информационна сигурност

Мерките, които могат да се предприемат за осигуряване на информационна сигурност, включват две основни групи решения – технологични и организационни политики:



Фиг. 1.4. Решения за осигуряване на информационна сигурност

Организационните политики включват одобрени политики, процедури, стандарти и указания, както и нормативна база и регулации. Целта им е да информират пер-

сонала за задължителните и забранените дейности в работния процес. Те формират базата от правила за реализирането на техническите мерки. Типичен пример за административни мерки са политиките за сигурност.

Технологичните решения предполагат използване на софтуерни инструменти, мониторинг и контрол на достъпа до информацията и компютърните системи. В тях се включват специализиран софтуер, контроли за осигуряване правата на потребителите за достъп до определени ресурси, шифриране и други. Съществено при логическия контрол е ограничаване на правата при използване на компютърна система. С този способ се предоставят нужните права за реализиране на поставените задачи.

Към посочените по-горе две групи решения могат да бъдат добавени и **физически**, които обхващат мониторинг и контролиране на работната среда, управление на достъпа, видео наблюдение, алармена инсталация, противопожарна инсталация и охрана. Съществен аспект на защитата на информацията при преработването и съхраняването ѝ в компютърните системи и предаването ѝ през мрежите включва физическата защита на окабеляването, комуникационната техника, сървърите и работните станции от неправомерен достъп.

7) Риск за сигурността на информацията в електронната търговия

За анализа и изясняването на този риск е необходимо да бъдат уточнени няколко съществени понятия – риск, уязвимост, заплаха и др. (Стоилов, 2011). **Заплахата** представлява действителна или латентна възможност за щети по отношение на информационните ресурси на организацията. Това може да бъде лице (нищо не подозиращ служител или злонамерен хакер), природно бедствие или общество от злонамерени лица. Всички изброени заплахи могат да доведат до пробиви в сигурността. **Уязвимостта** е слабост, от която може да се възползва злонамерено лице. При разглеждането на всички аспекти на информационната сигурност стигаме до извода, че броят на уязвимите места е много голям. Като уязвимости можем да посочим липсата на физическа защита на помещенията, в които функционират сървърите, стартирани ненужни услуги върху сървърите, нередовно архивиране на данни и др. Използването на лесни за компрометиране пароли създава сериозна уязвимост, която може да се елиминира със задължаването на потребителите да използват по-сложни пароли, които пък могат да се окажат трудни за запомняне и това да доведе до нова уязвимост. **Рискът** се определя като възможна **заплаха**, появила се поради **уязвимост** в системите чрез които се осъществяват електронните транзакции.

В случай, че заплаха се възползва от уязвимост, налице е риск, на който трябва да се противодейства. Обобщавайки посоченото по-горе, можем да формулираме:

$$\text{Заплаха} + \text{Уязвимост} = \text{Риск} \text{ (Threatanalysis, n.d.)}$$

Когато една компания търпи загуби вследствие на заплаха, настъпва **реализация на риска** (употребява се също и терминът „излагане” (**exposure**)). Реализацията на риска е явлението, от което компаниите се стараят да се предпазят след като са разбрали за наличието на връзка между заплахата и уязвимостта.

За редуциране на вероятността за реализиране на даден риск е необходимо да бъдат предприети **мерки за противодействие**. Заплахите от своя страна представляват потенциални опасности от различен тип, които е невъзможно да бъдат изцяло елиминирани и с тях трябва винаги да се съобразяваме.

Може да систематизираме, че върху уязвимостите съществува възможност за осъществяване на контрол, докато по отношение на заплахите такъв контрол не може да се реализира, те трябва да подлежат на анализ и въздействието им да се взема предвид.

В заключение може да обобщим, че за ЕТ съществуват редица схващания, но най-общо тя представлява осъществяване на сделки по електронен път, без пряк контакт между участниците. Чрез нея на компаниите се предоставят множество възможности за

повишаване ефективността на бизнеса, посредством навлизането му в Интернет. Темпът, с който се развива електронния пазар, налага на всяка организация активно присъствие в Интернет с електронен магазин или с предлагането на различни услуги, което да увеличи нейната конкурентоспособност. Осъществяването на ЕТ крие множество рискове, на които трябва да се отдели сериозно внимание и ресурси за тяхното поддържане в нормални граници, което да осигури естественото протичане на транзакционните процеси.

Информационната сигурност в системите за електронна търговия се свързва с осигуряване и поддържане на конфиденциалност, интегритет и достъпност на данните, без значение в какъв формат са представени - в електронен вид, физически, ръкописни или други. Тя се различава от компютърната сигурност, която има отношение към конфиденциалността, интегритета и достъпността на компютърната система, без да прави разлика дали съществува връзка с информацията, която се съхранява или се преработва от дадена система.

Ключовите компоненти на информационната сигурност - конфиденциалност, интегритет и достъпност се анализират спрямо трите основни елемента на компютърните системи - хардуер, софтуер и средства за комуникация. По този начин се цели да се разработят и имплементират стандарти за информационна сигурност като инструменти за сигурност и превенция на три нива - физическо, персонално и организационно. Процедурите и политиките за сигурност в СЕТ се формират с цел да се насочи персоналът към правилните начини за използване на информационните продукти и да се осигури информационната сигурност в бизнес организацията.

1.1.2. Проблемът на защитата на информацията и сигурността в електронната търговия

1) Причини за изследване на сигурността в електронната търговия

Придържането на информационната сигурност на високо ниво произтича от огромното значение, която тя има за нормалното функциониране на процесите в организацията. Нахари и Крутз разглеждат сигурността като съвкупно наименование на множество съществуващи защитни механизми по отношение на даден ресурс, както и тяхната ефективност (Nahari, 2011). От тази гледна точка за различни системи, прилаганите механизми за защита за ресурсите и тяхната ефективност също е различна. На практика механизмите за защита и степента на прилагането им са функция на заплахите към ресурсите. Както беше отбелязано, заплахата представлява потенциална възможност на неопределен субект да се възползва от специфична уязвимост, а атаката се разглежда като целенасочено действие срещу имплементирания механизъм за защита с цел използване на дадена заплаха, свързана с конкретен ресурс. От тук следва изводът, че когато няма ценност, която да се защитава, е безпредметно да се прилагат механизми за защита.

По отношение на ЕТ, при която една форма на стойност се заменя с друга, ресурсите, които са уязвими и е необходимо да се защитят, представляват данните за участниците в транзакцията, като данни за кредитни карти и онлайн идентичност. Защитата им е наложителна, понеже получаването на неоторизиран достъп от външно лице върху тях може да причини множество финансови, социални и други щети. Целевите системи и комуникационните инфраструктури, чрез които се взаимодейства в процеса на извършване на електронните транзакции имат значение както за потребителите, така и за системните оператори, и по тази причина към тях трябва да се приложат ефективни защитни механизми за защита от атаки.

Сериозни рискове носят със себе си сайтовете за колективно пазаруване, в които се предлагат продукти и услуги, най-често със значително намаление. Тези сайтове рядко извършват нелоялна търговска практика, като осигуряват платформа на търговци

за публикуване на некоректна информация, свързана с промоционална цена или стойност на отстъпката, която потребителят може да получи при закупуване на стока или услуга през сайта (Янкова, n.d.). Често срещана практика при тези електронни магазини е привличане вниманието на клиентите с отстъпка от 50% или повече, като в същото време съществува вероятност посоченото намаление да не бъде получено.

Основните проблеми са резултат от липсата на информация, позволяваща идентификацията на търговеца, което възпрепятства клиентите да упражнят правото си за връщане на закупената стока в законовия срок от 7 работни дни. Като допълнение, съществува възможност търговецът да не предостави информация, свързана с правото на отказ или за начина, по който то следва да бъде упражнено. Друг проблем при сайтовете за колективно пазаруване е използването на заблуждаваща търговска реклама, включващо предоставяне на невярна, съществено важна за потребителя информация, която оказва влияние върху вземането на решение за извършване на покупка.

2) Предиизвикателства пред постигането на висока степен на сигурност в електронната търговия

През последните години глобалните продажби чрез ЕТ нараснаха значително и се очаква тенденция на ускоряване на този растеж. Заедно с това развитие се увеличава и броят на измамите и престъпленията, извършвани по електронен път. По данни на Ponemon Institute (СЮ, 2012), средните годишните загуби на американски организации, причинени от киберпрестъпления възлизат на 8,9 милиона долара, което е увеличение от 6% спрямо отчетените загуби за 2011 г. и от 38% спрямо тези през 2010 г. Проучването за 2012 г. установи също и че има 42% увеличение на кибератаките. Тревожна е нарастващата резултатност на атаките - от 10 успешни атаки на седмица през 2010 г., на 72 за 2011 г., до 102 за 2012 г.

При извършване на електронна транзакция има **три потенциални ключови** точки на уязвимост, на които трябва да се обърне внимание. Те са **клиентът, сървърът и съобщителните канали**.

Основните проблеми в ЕТ, от гледна точка на клиента, са свързани с доверието и сигурността в процесите по електронен обмен на информация (Economy.bg, n.d.).

Осигуряването на високо ниво на сигурност е съществен проблем, който оказва влияние на потребителите при пазаруване онлайн. Потребителите обикновено са резервирани при предоставяне на своята лична финансова информация за осъществяване на онлайн сделката, защото се страхуват, че може да бъде прихваната от злонамерени лица при предаването.

Основните опасения на клиентите по отношение на сигурността при пазаруване в Интернет са свързани с *конфиденциалността, политиката на връщане на стоки, онлайн плащанията, опасност от предаване на вируси и присъствието на съответен сертифициращ орган, който да следи и гарантира тези сделки* (Shahibi S., 2011).

Потребителите пазаруват по-сигурно, когато има ясна **политика на търговците**, че след покупка продуктите могат да бъдат върнати, в случай че не са доволни. Минималното изискване при наличие на такава политика е, че съществува някаква форма на гаранция от страна на продавача, че качеството на продукта им е на ниво и е способен да отговори на изискванията на клиентите.

Основните проблеми на сигурността са свързани с **гарантирането на конфиденциалност на информацията**. При извършване на електронната транзакция потребителите са длъжни да предоставят личните си данни. Това може да бъде използвано неправомерно от търговците с цел продажба на тази информация на трети страни (други производители за пазарни цели). Предоставянето на гаранция от страна на

продавачите, че личната информация се третира добронамерено и е поверителна, създава в потребителите сигурност и положително отношение към онлайн транзакцията.

Защитата от зловреден софтуер при пазаруването онлайн е следващият елемент на информационната сигурност. При разглеждането на сайтовете на различни онлайн магазини, в персоналните компютри на потребителите се записват така наречените „бисквитки” (cookies). Тези малки файлове позволяват на сайтовете да следят страниците, които потребителите посещават и да изпращат информация. Това крие рискове, елиминирането на които се постига с конфигуриране на адекватни настройки за тяхното действие. Съществуват и опасни сайтове, които предават вируси, ако потребителите не приемат предложението им за закупуване на продукта. Това се окачествява като сериозна заплаха.

Сигурни онлайн плащания. При извършване на онлайн плащания, потребителите трябва да предоставят информация за кредитни карти, както и кода за сигурност, който е свързан с тях. Съществува риск от прихващане на тези данни от злонамерени лица и неправомерно използване на потребителските кредитни карти. Затова осигуряването на сигурни методи за онлайн плащане с високи нива на безопасност е от решаващо значение за изграждането на доверие към търговията през мрежата.

Следващото важно изискване на потребителите към онлайн търговията е наличието на **официален орган**, към който да се отправят жалби относно извършваните транзакции. Сделките в ЕТ са безлични и потребителите нямат достъп до продукта, който ще бъде закупен. Наличието на организации, към които да бъдат насочени всички жалби и които да осигурят следпродажбено обслужване допринася за засилване на увереността у потребителите, че пазаруват сигурно.

Създаването и използването на сигурна онлайн **комуникационна връзка** е сложна задача, изискваща сериозни ресурси. Съществуват редица технологични концепции, които осигуряват гаранция за достигането на изпращаните съобщения единствено до получателите, като една от основните идеи на технологиите е те да са достъпни.

За защита на **електронната поща** се прилагат множество разпространени механизми, в които се включват цифрови сертификати за удостоверяване на подателя на съобщенията, както и криптиране. При **чат програмите** обаче, все още няма достатъчно средства за защита. Различните опции включват използване на механизъм за удостоверяване на подателя и получателя на съобщението и използване на сигурен комуникационен канал, който да осигурява криптиране на информацията, така че в случай че попадне в трети страни, да няма възможност за разшифроване.

Посочените проблеми могат да бъдат разрешени с прилагането на стандартизирана клиент-сървър технология, като платформата **Jabber** (Димитров, 2010). Тя представлява протокол за пренос на текстови съобщения и съобщения за състояние, който е разработен като свободен стандарт и е базиран на Extensible Markup Language (XML). В последствие протоколът бе преименуван на **Extensible Messaging and Presence Protocol (XMPP)**. Употребата на този протокол в Интернет може да се приеме като решение за повишаване на сигурността на комуникациите. Пример в тази насока е Google, която използва XMPP като инфраструктура за чат програмата си Google Talk.

Последната ключова точка на уязвимост е **сървърът**. Защитата на сървъра е неделима част от изграждането на цялостна мрежова защита на организацията, защото сървърите съхраняват значителна част от информацията на компанията и евентуалното ѝ попадане в хакери и неоторизирани лица може да доведе до сериозни щети. Уязвимостите по отношение на сървърите, за които е необходимо предприемане на мерки за сигурността, са: неизползваемите услуги и отворени портове; невнимателно

администриране; използване на несигурни услуги (A Guide to Securing Red Hat Enterprise Linux, 2013).

От изброените проблеми става ясно, че на сигурността на ЕТ трябва да се обърне сериозно внимание и да се отделят средства.

В обобщение, можем да заключим, че в развиващия се електронен пазар, където всеки онлайн потребител е важен за успеха на дадена организация, осигуряването на високо ниво на информационна безопасност е основен и жизненоважен приоритет в СЕТ. В условията на цифрова икономика и повсеместното използване на Интернет, успешното взаимодействие с потребителите е немислимо без внедряването на техники, технологии и процедури за повишаване нивото на информационната сигурност, което би довело до стратегически предимства за внедряващата ги организация.

1.1.3. Предизвикателства пред сигурността в мобилната електронна търговия

Мобилните електронни устройства, от една страна, могат да бъдат използвани от потребителите в службата, в къщи и в движение за достъп до електронни магазини и извършване на покупки на стоки, а от друга, те могат да се използват от специалистите, поддържащи електронния магазин.

Мобилната е-търговия е нова сфера, възникваща от свързването на ЕТ с набиращите скорост мобилни и широко разпространени безжични технологии. Те се налагат като по-предпочитан метод за достъп до мрежата. Според проучване, проведено през 2012 г., 81% от притежателите на смартфони използват Интернет през мобилните си устройства (Груев, n.d.). Някои експерти твърдят, че това е основната причина сайтовете за ЕТ, които са оптимизирани за мобилен достъп, да осъществяват по-успешни продажби, въпреки че средната цена за транзакция от преносимо устройство е с 12% по-висока, от тази през настолен компютър. Независимо от това, много от клиентите предпочитат да разглеждат интернет сайтове чрез смартфони. Освен че предоставя всички предимства на ЕТ, мобилността на клиентите им осигурява преимущества и в случаите на традиционно пазаруване, защото клиентите могат веднага да проверят за по-добри възможности и по-изгодни цени, предлагани от други търговци.

Бързото навлизане на мобилната търговия затруднява анализирането на различните технологични проблеми, които тя поражда, и по-специално на тези, свързани със *сигурността* и *конфиденциалността*.

Поради спецификата на мобилните устройства да са отворени към безжични мрежи, сигурността на тези устройства в процеса на мобилната търговия, е много по-критична в сравнение с използването на настолни компютри. Много от рисковете, свързани с мобилни устройства, се пораждат от характеристики, които се определят като тяхното най-съществено предимство - преносимост и портативност. Мобилните устройства предават данни чрез безжични мрежи, които по принцип са по-несигурни от фиксираните мрежи и по този начин информацията може да се изложи на риск от прихващане. Значителна част от мобилните устройства притежават възможност за съхраняване на некриптирани данни за по-продължително време, което води до компрометиране на ценна поверителна информация, в случай на кражба или загубване на устройството. Освен това преносимите устройства са изложени на риск от разпространение на зловредни приложения, след което могат да бъдат използвани като платформа за вредителски действия. За сигурното използване на мобилни устройства е от първостепенно значение да се намери решение на посочените проблеми. Необходимо е да бъдат преразгледани традиционните компютърни комуникации в ЕТ, за да се гарантира, че приложението на мобилни устройства при извършване на електронни

транзакции, е защитено и се осъществява ефективно. Най-честите заплахи за мобилни устройства са представени в таблица 1.1.

Таблица 1.1

Заплахи и уязвимости, свързани с мобилните устройства.

Уязвимост	Заплаха
Данните преминават през безжични мрежи, които са по-несигурни от фиксирани.	Злонамерени външни атаки могат да навредят на организацията.
Мобилните устройства позволяват на потребителите да напускат границите на организацията и по този начин се елиминират много от мерките за сигурност.	Мобилните устройства излизат от границите на корпоративната мрежа и достигат до мрежови периметри, пренасящи зловреден софтуер, след което този софтуер може да проникне във вътрешната мрежа.
Съхраняване на некриптирана информация в мобилното устройство.	При прихващане на данните от външно злонамерено лице, или в случай на кражба, данните могат да бъдат прочетени и използвани неправомерно.
Използването на Bluetooth технологията е много удобно за потребителите с възможността за провеждане на разговори със свободни ръце, но много често Bluetooth оставен включен е откриваем.	Злонамерени лица могат да открият устройството и да предприемат атака.
Мобилното устройство няма включени изисквания за идентификация	В случай на загуба или кражба, външни лица могат да придобият достъп до устройството и всички данни, които то съхранява.
Организацията не може да управлява устройството.	В случай, че няма мобилна стратегия и политика, служителите могат да използват техните собствени устройства. Съществува възможност те да не могат да се свържат с виртуалната частна мрежа (VPN), но в същото време да им е позволено да взаимодействат с електронна поща и някои уязвими документи.
Устройството осигурява възможност за инсталиране на неидентифицирани и неподписани приложения.	Инсталираните неидентифицирани и неподписани приложения могат да съдържат зловреден код, който да се разпространява. Устройството може да бъде трансформирано в портал за вход към вътрешната мрежа на външни злонамерени лица.

На практика, използването на мобилните устройства може да представлява значителен риск за цялостната система за сигурност както на предприятието, така и на потребителя. Мобилните устройства имат множество точки на уязвимост, които могат да бъдат обект на злонамерени атаки, както и на съзнателни вътрешни заплахи.

Тъй като мобилните устройства все повече се налагат като важен инструмент в бизнес операциите, много съществено за сигурността е да се обмисли как да се управляват рисковете, свързани с тези устройства. Решаването на проблемите със

сигурността ще гарантира на потребителите тяхната автентичност, цялостност на данните и доверие в устройството.

Според нас, това може да стане чрез прилагане на редица мерки като:

- отдалечен контрол на устройството с цел то да може да бъде проследено;
- сигурни методи за удостоверяване на потребителя като ПИН код, пароли и други защити;
- криптиране на данните в мобилните устройства така, че информацията да е неизползваема, в случай на кражба;
- криптиране и привилегиран контрол до достъпните системи;
- следене и ограничаване на прехвърлянето на данни към джобни и преносими устройства от една единствена точка;
- информиране на потребителите за най-новите и най-сигурните устройства;
- отчетност, отговорност и прозрачност при използване на устройството;
- регулиране на устройствата от инсталирането им до излизането им от употреба.

Можем да обобщим, че мобилната търговия се развива с много бързи темпове и пазаруването чрез мобилни устройства все по-често се среща при масовите потребители. Широкото разпространение и използване на мобилните устройства ги прави обект на постоянен интерес, както за обикновения потребител, така и за злонамерени лица с цел насочване на атаките към тях. От изключително значение е да се намери правилен подход за решаване на проблемите със сигурността в мобилната търговия. С решаването на тези проблеми потребителите ще добият повече увереност да пазаруват по този начин, а това пък от своя страна ще доведе до много сериозен темп на развитие на мобилната търговия в бъдеще.

1.2. Защитата като нефункционален компонент на системата за електронна търговия

1.2.1. Значение на защитата за функциониране на електронната търговия

Поддържането на информационната сигурност на една развита СЕТ е комплексен процес, който включва идентифициране на всички точки на уязвимост в системата и прилагане на адекватни защитни механизми за повишаване нивото на сигурност в слабите места с цел да се осигури оперативният интегритет.

Процесът на защитаване на системата започва с идентифициране на факторите, които въздействат върху уязвимостите на системата за ЕТ за атаки и последващо внедряване на механизми, които да ги контролират. Описаният процес налага задълбочено познаване на ценните ресурси, изискващи защита, както и потенциалните атаки, на които те са изложени. В ресурсите на ЕТ, на които винаги трябва да се осигури защита, се включват данните, които потребителят трябва да въведе при автентификация и оторизиране в системата за ЕТ като потребителски имена, пароли и др. Много важно за защитата също е контролирането на действията, които даден оторизиран потребител може да извършва. Съществува категория атаки, наречена „ескалиране на привилегиите“, където оторизирани потребители с ниски привилегии получават достъп до системата и се възползват от слабости в защитата с цел достигане до определени ресурси. Освен това сериозна защита се изисква и за съхраняваните данни в базите данни (данни в покой - Data-at-rest - DAR) и за данните, които се предават по комуникационните линии (данни в трансфер – Data-in-transit, DIT) (Nahari, 2011).

Разгледаните дотук аспекти дават представа за техники, които повишават защитата в ЕТ – оценка на уязвимостите, анализ на заплахите, автентификация,

оторизиране и защита на данните в покои и в трансфер. Съществуват други две, все още фундаментални концепции, без които защитата на ЕТ е немислима: **сигурност на слоеве и защита в дълбочина**. Всяка ефективна, мащабируема, разширяваща се и гъвкава система въплъщава тези концепции при дизайна и внедряването на механизмите за сигурност. Формирането на различни нива на сигурността в отделните елементи на инфраструктурата на организацията разпределя обхвата на сигурността и я прави ефективна. По този начин се избягва излагането на единична точка на срив на системата, което оказва положително влияние върху ЕТ.

При внедряването на защитни механизми трябва да се вземе предвид, че сигурността не е статична и не се изчерпва с прилагането на описаните техники за автентификация, оторизация и формиране на слоеве на защитата. На практика не е възможно да се идентифицират напълно всички уязвимости на системата за ЕТ и по тази причина не е възможно те да бъдат изцяло защитени. Освен това характеристиките на даден обект, които определят необходимостта му от защита могат да се променят с течение на времето. Така е и при връзките на обекта с други обекти. Следователно идентифицирането на обектите за защита и прилагането на съответни защитни механизми за тях е задължително. Колкото по-активно е присъствието в Интернет, толкова по-сложни ще бъдат процедурите по идентифицирането на уязвимостите и мерките за осигуряване на защитата им. Това прави процеса по гарантиране на сигурността сложен комплекс от дейности, като той засяга в най-голяма степен операционните и експлоатационните аспекти на системата за ЕТ.

1.2.2. Рискът като ключов фактор в информационната сигурност на електронната търговия

Сигурността, определяна и зависеща от риска, е модерна и съвременна концепция. Един от основните стълбове на ЕТ е управлението на риска от операционна, транзакционна и финансова гледна точка и цялостно във всички аспекти от неговата функция (Nahari, 2011). Разбирането на концепцията за сигурност, определяна и зависеща от риска, налага дефинирането на понятието риск в този контекст. Рискът може да се дефинира като математическа вероятност дадено събитие да настъпи, или да бъде предотвратено в бъдеще, от колкото настоящ проблем, който да причини щети.

Концепцията за сигурност, определяна и зависеща от риска, се основава на дизайн и използване на мерки, базирани на вероятността дадена атака да се осъществи. Съществува значителна разлика между дизайна на статичната сигурност и динамичната, изискваща незабавно предприемане на адекватни действия в мащабируеми системи като тази на ЕТ.

Гарантирането на сигурността на организацията ѝ коства множество ресурси и време. Всяко реализирано действие, свързано със сигурността, предполага наличието на финансови, технически и човешки ресурси. По отношение на сигурността на системата на ЕТ, от значение е точното измерване на риска за загуба или компрометиране на ресурсите и на тази база да бъдат внедрени защитни механизми за предпазване на рисковите ресурси от тези заплахи. Начинът на действие на защитните механизми се определя от ресурса и асоциирания с него риск – именно в това се изразява модерната концепция за сигурност, определяна и зависеща от риска. Типичните критерии за оценка на риска включват пари, време, място и др., правещи я значително по-ефективна и точна.

Използването на математически модели и правила при оценяването на рисковете прави прилагането на концепцията за сигурност, определяна и зависеща от риска, силно зависимо от данните. Пример за това е свързването на даден потребител към онлайн магазин и извършване на покупка. С извършването на заплащането, потребителят

въвежда данните си, чрез което системата на електронният магазин засича логическия адрес на потребителския компютър в дадено местоположение. При условие, че след известно време (няколко часа) същите данни на потребителя бъдат коректно засечени и посочат местоположение, различаващо се драстично от предишното, инфраструктурата на сигурността, определяна и зависеща от риска блокира потребителския акаунт и предприема последващи действия, базирани на коректните потребителски данни. В този случай се изисква лимитиран набор от данни, отнасящи се до местоположението. Възможни са много по-усложнени ситуации, като предприемането на плащане през дадена електронна разплащателна система, което може значително да се различава от предходните навици за плащане на потребителя. В този случай системата за електронни разплащания не е в състояние да определи дали транзакцията е достоверна или е активност с цел измама. Описаният пример е доказателство, че при вземането на решения, базирани на сигурност, определяна и зависеща от риска, са необходими огромно количество данни и добре разработени модели за оценка на риска. Те трябва да осигурят безпроблемно обслужване на легитимните потребители и в същото време да е възможно да се предприемат действия срещу неоторизирани активности.

В заключение стигаме до извода, че сигурността, определяна и зависеща от риска е изключително мощен компонент от напредналите техники по отношение определяне нивото на сигурност. Тя представя философия, основана на вероятността от атаки към ресурсите и оптимизира приложението на мерките за противопоставяне на дадените уязвимости. Внедряването на ефективна система за сигурност, определяна и зависеща от риска извежда на преден план проблема с рисковете, като добавя динамични и ресурсно-ориентирани възможности за справяне с тях.

1.3. Подходи и решения за поддържане на информационната сигурност в системите за електронна търговия

1.3.1. Основни аспекти на защитата в електронната търговия

1) Защита и използваемост на системата за електронна търговия

Съществува схващането, че повишаването на сигурността в една СЕТ води до понижаване на използваемостта на системата. На практика това не винаги е така. Съществуват креативни защитни механизми, които не оказват пряко въздействие върху използваемостта на СЕТ, като мерки, базирани на местоположението, които са проектирани да нямат влияние върху използваемостта ѝ. Също така, за разлика от сигурността, където всяко действие е с определена цена, при използваемостта на СЕТ е възможно такава цена да не съществува (Nahari, 2011).

В СЕТ повишаването на сигурността се осъществява с прилагането на стандарти, технологии и вътрешни правила и процедури относно пароли за достъп, начини на предаване на информацията и др.

2) Пароли за достъп

Глобалната мрежа е замислена и проектирана като средство, което да свързва хора и системи с некомуниална цел. Поради това комуникациите чрез Интернет са отворени и не могат да бъдат контролирани, което е в противоречие с процесите в ЕТ, където се изисква конфиденциалност и цялостност на транзакциите. Все по-широкото използване на Интернет в бизнеса и налагането на глобалната мрежа като средство за извършване на комерсиални транзакции поставя проблема на сигурността на преден план.

Един от главните проблеми в Интернет е свързан с **идентификацията на потребителите**. За да се гарантира информационната сигурност е нужно да се избягва нераз-

решен достъп, както до данните, така и до критичните за бизнеса системи в дадена компания. Последниците от този достъп могат да бъдат модифициране, заменяне, разпространение или унищожаване на определена информация.

Технологията на **потребителското име** е най-масово използваната за идентифициране в многопотребителските компютърни системи и мрежи (Сигурност и защита на информацията в Интернет - Идентификация на потребителя, n.d.). Потребителското име, наричано още потребителски акаунт или име за свързване, е средство за установяване на самоличност и правомощие за достъп до даден компютър или мрежа. Влизането с определено потребителско име и парола осигурява различни права за достъп.

Потребителските пароли по правило трябва да са стабилни, достатъчно дълги, трудни за отгатване от външни лица, но не толкова трудни за помнене и включващи символи, различни от буквите в азбуката и числата, също така и микс от малки и главни букви и трябва да бъдат често променяни (Nahari, 2011). Принципно човешката памет е с ограничен капацитет. На практика повечето потребители избират слаба парола за достъп до най-често посещаваните сайтове, за да става достъпа по възможно най-бърз начин и без никакви пречки. Това значително намалява ползите от паролите като мярка за сигурност.

3) Потребителски интерфейс

Като се има предвид ефективността на мерките за сигурност, които да се изберат, трябва да се направи връзка между използваемостта на предложените решения и опита на потребителите. Това налага да се осъществи тясна връзка между специалистите по сигурността, опита на потребителите и дизайнерите на потребителския интерфейс през целия жизнен цикъл на продукта в ЕТ. На практика, ако мерките за сигурност имат интерфейс към потребителите и изискват взаимодействие с тях, те следва да бъдат валидизирани като методи, основани на потребителите. Подобни методи имат възможност да покриват различни групи по възраст, различни целеви групи и потребителите в различни локации, за да се гарантира, че аспектите на използваемостта на решенията за сигурност са добре отчетени и това е допринесено от лесното приспособяване към тях (Nahari, 2011). Важно е да се обърне внимание на интерфейса за мобилните приложения, поради масовото използване на преносими устройства. В тази насока, при проектирането на интерфейса и структурата на сайтовете, основните направления трябва да включват независимост по отношение многобройните екранни резолюции, както и възможността за лека и плавна навигация чрез докосване или така наречените тъч интерфейси.

Като препоръки към мерките за сигурност при дизайна на електронния магазин можем да посочим осигуряване на електронни сертификати като Hacker Safe или VeriSign и актуализиран SSL сертификат, за да се изгради доверието на клиентите и да се предлага по-високо ниво на сигурност при пазаруване.

4) Защита и мащабируемост

Създаването на сигурна СЕТ и използвани механизми за защита и автентификация е безсмислено без постигане на високо ниво на мащабируемост. Целта на дизайна на мащабируемостта е да се идентифицират всички пропуски в системата и те да бъдат елиминирани. Най-често това се постига с внедряването на определени принципи, в които се включва: елиминиране на единствена точка на отказ, абстракция на основните функции, възможност за едновременно изпълняващи се процеси, прилагане на асинхронни операции и др. От друга страна, при проектиране на сигурността, вниманието е насочено към защитата на информационните ресурси и потенциалните атаки и заплахи, на които те са изложени. Комбинирането на двете методологии довежда до формирането на сигурност, основана на определено ниво на мащабируемост.

Основна пречка пред сигурността, основана на определено ниво мащабируемост, е осъществяването на тясна връзка между функционалността на механизмите за информационна сигурност и бизнес логиката. Такъв пример може да бъде процесът на автентификация, който изисква собствена подсистема, действаща самостоятелно и независимо от главната система. Практиката показва обаче, че съществуват множество примери за системи, в които се преплита логиката на автентификацията и бизнес логиката. Проектирането и прилагането на една система по този начин е безцелно, понеже разсъжденията относно програмната логика са изключително трудни. Това важи и при въвеждането на определено ниво на мащабируемост - функционирането на система, включваща бизнес логика и механизми за сигурност в нейния дизайн и имплементация прави въвеждането на мащаб изключително предизвикателство.

Важността на дизайна на мащабируемост на сигурността добива по-високи измерения, когато се отнася до информационната сигурност в СЕТ. Всеки електронен магазин отчита период на засилени атаки, при което различни части от защитната инфраструктура трябва да бъдат подсилени, за да може да се противодейства на атаките и в същото време легитимните потребители да могат да осъществяват достъп. Пример за такъв сценарий е атака тип разпределена атака отказ от услуга (Distributed Denial Of Service – DDOS).

5) Защита на транзакциите

От гледна точка на ЕТ, транзакцията може да се определи като свързване на програмна функционалност, мениджмънт на процесите, взаимодействие между потребителите и обмяна на стойности. За подсигурияването на дадена транзакция е необходимо да се изгради сигурност на всички отделни нейни компоненти и това трябва да стане синхронно. Подсигурияването на транзакцията започва от реализирането на връзка със СЕТ и продължава с всяка индивидуална стъпка през целия процес, като за всяка от тези стъпки трябва да бъдат приложени ефективни механизми за сигурност. В противен случай транзакцията не може да бъде считана за сигурна. На практика това означава, че не само информационните ресурси, които участват в транзакцията, трябва да бъдат защитени, а също и характеристиките на целия процес при извършването му. За извършване на електронни транзакции предлагаме да се използват протоколите за сигурна връзка SSL и SET (вж. глава 3 т. 3.3.4).

б) Дефиниране на минимално ниво на сигурност

Подсигурияването на електронната транзакция не приключва с нейното изпълнение. В много случаи електронните транзакции изискват да се приложи механизма на неотричане на сделката. Друг аспект от защитата на транзакциите е поставянето на подходящи протекционни мерки, които са пропорционални на заплахите и рисковете към СЕТ. Това означава, че няма нужда транзакционните данни да бъдат криптирани, докато в тях не бъдат включени чувствителни данни. Обобщено казано, достатъчното осигуряване на транзакциите се изразява в защитата им от причинни, практически и вероятностни атаки.

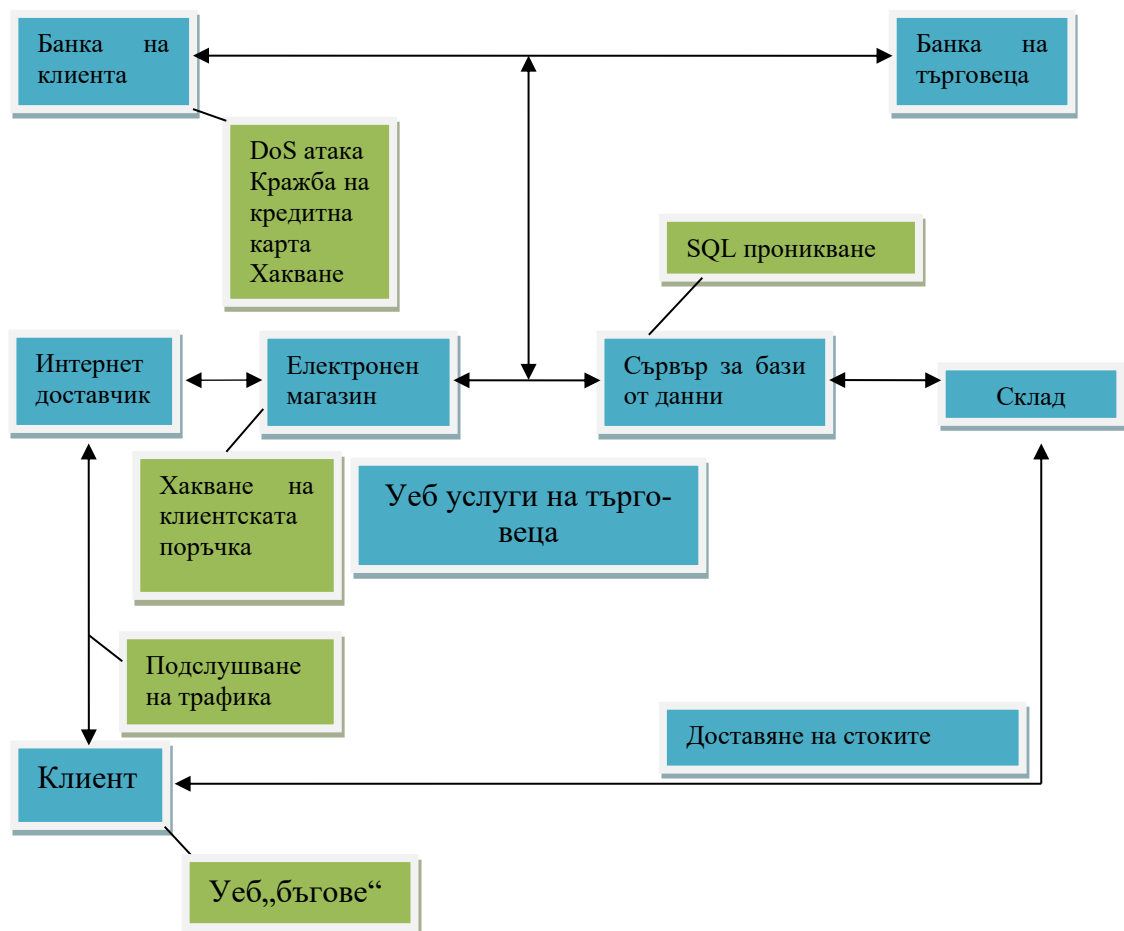
От казаното до тук е ясно, че ЕТ обединява много технологии в себе си, като предлага улеснение на своите потребители. ИТ непрекъснато еволюират и това освен положителни, има и отрицателни страни. Колкото повече се развиват съвременните ИТ, толкова повече възможности те предоставят. Тези възможности могат да се използват добронамерено за нуждите на потребителите, или умишлено от злонамерени лица за осъществяване на измами и други нарушения. Поради тази причина осигуряването на защита на информацията е едно от големите предизвикателства към съвременните информационните и комуникационни технологии. Затова може да се направи изводът, че раз-

решаването на проблема със сигурността на ЕТ, а именно гарантирането на конфиденциалност, цялост, наличност, легитимност и липса на отказ от данните, изисква спазване на строги правила, които гарантират безопасността на информацията при оперативните дейности.

1.3.2. Систематизиране на заплахите в електронната търговия

Процесът на извършване на ЕТ може да се представи в 4 стъпки: информиране, договориране, доставка на закупената стока и сервиз и поддръжка (Върбанов Р. , 2009). Във всеки един от тези етапи съществуват потенциални заплахы, които могат да попречат на нормалното извършване на сделката (вж. фиг.1.5).

В настоящия анализ на проблемите за сигурността в ЕТ ще систематизиране споменатите по-горе заплахы, базирайки се на трите потенциални ключови компоненти на уязвимост на електронната транзакция, особено в точките им на свързване, а именно споменатите в т.1.1.2 - клиент, сървър и съобщителни канали.



Фиг. 1.5. Точки на уязвимост в ЕТ транзакция, източник: адаптирано по (Laudon К. Т., 2013)

Най-общо заплахите за информационната сигурност могат да се обособят в няколко групи (Роров, 2014):

- **вредителски код** (malicious code / malware) - вируси, троянски коне, червеи, Drive by download, bot, backdoor;

- **потенциално нежелана програма (PUP)** - adware, spyware и др.;
- **фишинг (Phishing)** онлайн опита за измама с цел придобиване на конфиденциална информация;
- **хакери и кибер вандализъм** - зловредна активност от *хакери, кракери, white hats, grey hats, black hats, data breach*;
- **кражби/измами с кредитни карти** – използване на картата от друго лице, кражба на данни за карта, кражба на самоличност;
- **spoofing** – заплаха, която се проявява, когато хакери се опитват да се представят невярно, вземайки чужд имейл адрес или се маскират като друг потребител;
- **атака отказ от услуга – Denial of Service attack (DoS) и разпределена атака отказ от обслужване – Distributed denial of service attack (DDOS)** – заливане на сайта с безполезен трафик с цел претоварване на мрежата;
- **sniffing** - вид подслушваща програма, която наблюдава информацията, преминаваща през мрежата;
- **вътрешни атаки** – атаки от вътрешните служители, които имат достъп до жизнено важната информация и процедури;
- **лошо проектиран свърърен или клиентски софтуер** - софтуерни дефекти и уязвими точки, произтичащо от нарастването на сложността и размера на софтуера;
- **проблеми със сигурността на социалните мрежи** – вредителски код, PUPs, фишинг, пробив в данните, кражба на самоличност и др., които са се разпространили в социалните мрежи;
- **проблеми със сигурността на мобилните устройства** – всички видове заплахи, типични за мобилните устройства за достъп до Интернет, както и редица нови рискове, свързани със защитата на безжичните мрежи;
- **проблеми със сигурността на облачните изчисления** - мигрирането на все повече интернет услуги към облака създава риск за сигурността.

Освен общите заплахи за информационната сигурност, посочени по-горе, има дефинирани класификации конкретно за системите за ЕТ, в зависимост от различни критерии.

Пълна класификация на видовете заплахи в СЕТ е предложена от Горшков (Горшков, 2003):

- вътрешни атаки от служители – служителите на компанията умишлено нанасят щети;
- проникване в системата през Интернет – външни атаки през глобалната мрежа;
- вирусни атаки – разпространяване на зловредни програми;
- отказ от обслужване (DoS) – невъзможност за заплащане или за завършване на поръчка;
- нарушаване целостта на данните или мрежите – манипулиране на предаваните данни по мрежата;
- повреда на персоналния компютър – неизправност в компютъра на потребителя;
- финансови измами – кражби на лични данни, номера на карти и използването им.

В зависимост от компонента на СЕТ, в който се проявяват, заплахите за сигурността могат да се обособят в пет големи групи (MehdiKhorsow-Pour, 2004):

- заплахи, свързани с комуникационната среда – използване на уязвимости на средата с цел подслушване на трафика;
- заплахи, свързани с техническите компоненти – повреди или умишлени намеси с цел извличане на поверителната информацията;
- заплахи, свързани с платежния процес – кражба на номера на кредитни карти, лични данни на потребителите и др.;
- заплахи, свързани с прилаганите криптографски методи и технологии – прилагане на некоректно изпълнени криптографски процедури за кодиране на данните;
- други видове заплахи.

Маринова също разглежда проблемите на сигурността при ЕТ и по-конкретно взаимодействието с клиенти, предлагайки мерки за справяне с тях (Marinova, 2012). Според нея, тези мерки включват:

- криптиране на отдалечените данни;
- мониторинг на безжичните връзки;
- сигурност, базирана на длъжностите в организацията;
- обучение на персонала;
- предпазване от фишинг.

Според нас особено полезно би било разглеждането на заплахите в СЕТ от гледна точка на основните взаимоотношения и връзки между участниците в ЕТ и по тази причина предлагаме класификация на заплахите в СЕТ, базирана на тези отношения. Основните взаимодействия, които можем да разграничим, са: **бизнес към бизнес, бизнес към доставчик на приложения, клиент към бизнес и отношения между страните на електронната транзакция**. Осъществяване на тези взаимодействия с високо ниво на сигурност разглеждаме в предложения архитектурен модел на СЕТ (вж. глава 3 т. 3.3.4). Заплахите, които могат да възникнат във взаимодействията между участниците в СЕТ са следните:

- клиент към бизнес – подвеждане на клиента, проникване в клиентския компютър и сканиране, фишинг, подслушване на мрежата между клиента и електронния магазин;
- бизнес към бизнес – подслушване на мрежата, манипулиране на съобщения;
- бизнес към доставчик на приложения – получаване на подвеждащи програми от злонамерено лице;
- отношения между участниците в електронната транзакция – прихващане на трансфера на данни относно банкови карти, пароли за достъп до сметки и др.

За предпазване на организационната инфраструктура от кибер атаки е създаден Консорциумът ISTF (Internet Security Task Force) (Maxstead, n.d.), чиято цел е разработване на технически, организационни и операционни ръководства и правила за безопасност. ISTF създава области на информационна безопасност, които трябва задължително да се вземат предвид от занимаващите се с електронен бизнес, за да осигурят работоспособност на своите системи (Върбанов Р. П., 2011):

- автентификация;
- право на персонала, частна или лична информация;
- правилно определяне на събитията, свързани с безопасността;
- защита на корпоративния периметър;
- определяне характера на атаките;
- контрол върху потенциално опасното съдържание;
- контрол върху достъпа;

- администриране;
- реакция на събитията.

С тези препоръки могат да се открият навреме пробивите в сигурността и да се противодейства ефикасно, с оглед предотвратяване на евентуални атаки.

След детайлното систематизиране на заплахите за ЕТ, можем да направим извода, че осъществяването на ЕТ е процес, който крие множество опасности от различно естество. Наличието на заплахи при отделните етапи от реализирането на сделките по електронен път, изисква мениджмънтът на организацията да обърне сериозно внимание на безопасността на критично важната информация. Поради факта, че все повече от нея се съхранява и обработва по електронен път и се предава в компанията през мрежи или Интернет, непрекъснато се увеличават рискът от неоторизиран достъп, атаките и опитите за злоупотреби, както нарастват и предизвикателствата по отношение на решаването на проблемите, свързани с тях.

Гарантирането на сигурността на информацията може да се осъществи като се избере правилен подход, стратегия или се следват общоприети стандарти за информационна сигурност.

1.3.3. Тенденции в развитието и заплахите за информационната сигурност на електронната търговия

Основните тенденции в развитието на ЕТ са посочени от главните оперативни директори на водещи европейски компании (Ecommercenews.eu, n.d.):

- **Непрекъснат ръст на мобилната електронна търговия.** През следващите години се очаква повечето онлайн магазини да предлагат и мобилен сайт, поради масовото разпространение на мобилните устройства и превръщането им в предпочитан начин за пазаруване. Резултатът от това няма да е социална медия, която да популяризира мобилната търговия, а по-скоро собствен онлайн маркетинг на продавачите.

- **Навлизване на масовите данни (Big data).** Онлайн продавачите на стоки и услуги ще насочат вниманието си към анализиране на потребителите и техните навици, за да са наясно с намеренията им. Целта е да се осигурят съответните оферти в подходящия момент и по този начин да се повиши ефективността на ЕТ.

- **Пазаруването става глобално.** Очаква се ориентиране на местните купувачи към чуждестранни и далечни електронни магазини и съответно извършване на трансакции и парични преводи по тях. Това би поставило сериозни проблеми пред местните онлайн продавачи, но от друга страна може да предостави възможности за продажби в чужбина.

- **Пресъздаване на присъствието в традиционен магазин.** С цел улесняване на клиентското решение, е необходимо купувачът да може да преглежда наличните предлагани стоки и да му се предоставя необходимата информация по начин, сходен с този при физическото присъствие в традиционен магазин. Това означава фокусиране върху знанието за предлаганите продукти чрез въвеждане на техники и интерактивни технологии, чрез които потребителите ще могат да задават въпроси към персонала дори онлайн.

- **Персонализация.** Електронният маркетинг под формата на електронни писма, реклами на електронни магазини, брошури и др. става все по-целенасочен. Презентирането и офертирането ще се ориентира към клиентските предпочитания, поведение и покупателна способност с цел максимизиране на продажбите, фирмената печалба и потребителската удовлетвореност.

Посочените тенденции оказват влияние и в тенденциите за заплахите за ЕТ. Отчитайки състоянието на пробивите в сигурността и състоянието на пазара през последните години, водещите доставчици на средства за защита на информацията, в лицето на Sophos, Symantec, Trend Micro и др., както и изследователски компании като IDC, Gartner и др., представиха прогнозите си за съществените тенденции в областта на информационната сигурност, според които заплахите се насочват към мобилните платформи, хактивизъм, социалните мрежи и др. Основните направления, към които ще насочим вниманието си в настоящото изследване включват социалните мрежи и Web 2.0 услугите, мобилните устройства, социалния инженеринг и вътрешните заплахи (CIO, Информационната сигурност – 13 тенденции за 2013 година, 2013).

- **Все по-широко използване на социалните мрежи и Web 2.0 услугите**

С откриването на ефективни инструменти за комуникация с партньори и клиенти, бизнесът проявява все по-голяма активност в социалните мрежи. Проучване, проведено от Panda Security (Кръстева, 2011), констатира засилено внимание към Web 2.0 от страна на киберпрестъпниците. Данните от проучването показват, че при 71,6% от респондентите Facebook е най-честата причина за заразяване с вреден код, а нарушаване на конфиденциалността е настъпило при 73,2%. На второ място по заразяване с вируси се нарежда YouTube с 41,2%, а най-много проблеми със запазване на конфиденциалността има в Twitter - 51%. Според същото проучване, за 62% от респондентите социалната мрежа Facebook е причина за изтичане на данни, Twitter – за 38%, YouTube - за 24% и LinkedIn – за 11%.

Според нас, като решение на проблемите в тази област може да се посочи въвеждане на забрана служителите да общуват в социални мрежи от работните компютри, а достъпът до такива популярни сайтове да се разрешава само при необходимост за изпълнението на служебни задачи от определени работни станции с ограничена свързаност към корпоративната ИТ инфраструктура. За тези станции е препоръчително спазването на следните процедури:

- редовно обновяване на софтуера;
- използване на сложни пароли;
- избягване на подозрителни линкове;
- повишено внимание по отношение на кибер измамите;
- избягване споделянето на конфиденциална лична и служебна информация;
- отхвърляне на съобщения за потвърждаване на лични данни;
- повишено внимание при инсталиране на приложения.

Ние считаме, че по отношение на сигурността също е необходимо да се осигурят условия за натрупване, обработка и съхранение на солидния обем информация, събран от сайтовете на социалните мрежи, за да може той да бъде използван пълноценно от търговците, както и да се предвиди обучение на клиентите и потребителите относно заплахите, свързани със социалните мрежи. Техниките и технологиите за предпазване на клиентите и електронните магазини от опасностите, свързани със социалните мрежи, са представени в архитектурния модел за СЕТ (вж. глава 3, т. 3.3.4).

- **Все по-масово използване на мобилни устройства**

Мобилните устройства, актуалният подход за ползване на ИТ услуги и възгледът за употреба на персоналните устройства в работата - Bring Your Own Device (BYOD) са един фрагмент от факторите, които оказват съществено влияние върху корпоративната система за информационна сигурност.

Търсенето и поръчката на стоки и услуги през мобилни устройства изисква да се разработят мобилни приложения, които да улеснят потребителите. Типичните заплахи за мобилни приложения включват подмамване за изпращане на съобщения или

обаждания към платени номера, блокиране на информация с цел изнудване, измами с мобилни реклами и др. (PCWORLD, 2014)

Според изследване на Forrester Research, възникват нови способности за защита (CIO, 4 Прогнози за мобилната сигурност, 2013). По данни на проучването, 70% от организациите имат изградена BYOD програма, 62% от сътрудниците използват в работата си смартфони, а 56% от използващите таблети са ги закупили самостоятелно. Резултатите от проучването дават основание за следните прогнози:

- личните устройства ще добият по-широка популярност;
- мобилната виртуализация при поискване се превръща във водеща насока при управление на мобилни устройства;
- корпоративните приложения на база HTML5 ще увеличат своята популярност;
- мобилните услуги, ориентирани към личността изискват повишено внимание към конфиденциалността на информацията.

За покачване нивото на сигурността се препоръчва персоналните устройства да бъдат включени в обсега на приетите стандарти за управление на достъпа. В допълнение организациите трябва да поставят фокуса на програмите си за осведомяване по въпросите на информационната сигурност и по проблемите, отнасящи се до концепцията BYOx (Bring Your Own Anything – донеси каквото искаш).

Като механизми за осъществяване на превенция срещу рисковете свързани с мобилни устройства можем също да посочим:

- сваляне на приложения само от официални източници;
- избягване отварянето на подозрителни линкове;
- избягване обществените Wi-Fi мрежи и задължително включване на устройството към VPN;
- инсталиране на мобилен антивирусен софтуер;
- избягване използването на критично важните приложения, напр. тези за мобилно банкиране, извън средата на защитената домашна или офис мрежа;
- актуализиране на мобилния софтуер до последната версия;
- да не се поставят отметки на опциите “неизвестни източници” и “режим на разработчик” в настройките на мобилното устройство;
- определяне на допустимите видове устройства;
- определяне на характера на услугите, достъпни чрез устройствата, като се вземе предвид съществуващата ИТ архитектура;
- определяне на начина, по който служителите използват устройствата, отчитайки корпоративната култура и човешките фактори;
- интегриране на всички издадени от предприятието устройства в едно приложение за управление на информационните ресурси;
- описание на вида на автентичността и криптирането, присъщи на устройствата;
- очертаване на задачите, за които служителите могат да използват устройствата и видовете приложения, които са позволени;
- изясняване на начина за сигурно съхраняване и предаване на данните.

Плащането чрез мобилни устройства също крие рискове от прихващане на еднократни пароли и получаване на достъп до банковите сметки на жертвите, както и кражба на устройството, блокиране на транзакции и др.

Като подходящи мерки, които могат да се използват, можем да посочим незабавна смяна на паролите за онлайн банкиране и за мобилни услуги след приключване на разплащането, както и протоколите за защитен безжичен достъп WEP, TKIP EAP и др.

Те са използвани в архитектурния модел за подсигуряване на връзката между клиентите и електронния магазин. Заплахите и решенията от този тип са представени в предложени архитектурен модел за СЕТ (вж. глава 3, т. 3.3.4, фиг. 3.39).

- **Опасности, свързани със социалния инженеринг**

Сериозен проблем в съвременното информационно общество е манипулирането на потребителите с цел получаване на конфиденциални данни – т.нар. социален инженеринг. С развитието на Интернет технологиите, мобилните комуникации и социалните мрежи, ескалацията на заплахите, причинени от социалният инженеринг, добиват разрастителни мащаби (Platzer, 2012).

Към края на 2012 г. потребителите на най-популярните социални мрежи Facebook, Google+, Twitter и LinkedIn са над милиард и половина и потенциалните възможности за въздействие върху тях са много и са трудно предвидими (Ebizmba, 2012). В България активните потребители само на Facebook са над 200 хил. и като се отчете огромният брой хора, които не използват компютър в ежедневието си, можем да направим предположението, че приблизително всеки втори ползващ компютър, посещава и социални мрежи, което носи множество сериозни рискове.

Основните опасности, имащи отношение към социалния инженеринг, са насочени към социални манипулации, революции (Ghannam, 2011) и негативно въздействие върху подрастващите (Bavelier, 2011). Отчитайки тези проблеми, можем да отбележим още два съществени момента:

- влиянието на маркетинговите кампании в социалния инженеринг;
 - потребителското мислене и активност в социалните мрежи (Scientists, 2012).
- Като мерки за успешна превенция на социалния инженеринг можем да формулираме:
- препоръчително е да не се предоставят данни под въздействие на емоционален афект;
 - желателно е наличието на скептично отношение към всякакви нежелани съобщения;
 - препоръчително е да не се отговаря на искания за финансова информация или пароли;
 - препоръчително е да се отхвърлят искания за помощ;
 - повишаване вниманието върху защитата от кражба на имейл профила;
 - препоръчително е да не се изтеглят файлове от непознати източници;
 - повишено внимание към оферти направени от външни финансови организации, като чуждестранни лотарии;
 - препоръчително е настройките за филтриране на спам съобщенията да бъдат зададени на високо ниво;
 - подсигуряване на компютърните устройства чрез инсталиране на антивирусен софтуер, антифишинг инструменти, защитни стени, филтри за електронна поща и редовно да се актуализират съответните приложения.

- **Вътрешни заплахи**

Вътрешните заплахи все по-осезаемо излизат на преден план и поради тяхната комплексност съществуват много причини, поради които намаляването им се счита за сериозно предизвикателство.

Опитите за противодействие на тези заплахи остават в по-голямата си част неуспешни, обобщава проучване, проведено от PwC, списание CSO, Секретната служба на САЩ, програмата CERT на Института по софтуерно инженерство към университета “Карнеги Мелън” и ФБР, в което са включени над 500 изпълнителни директори в САЩ,

експерти по сигурността и други специалисти от частния и обществен сектор (CIO, Вътрешните заплахи - технологиите не могат сами да решат този проблем, 2013). Според проведеното проучване, 17% от анкетиранияте, които са били обект на вътрешна атака, не са наясно до какви последствия е довела тя, 33% от респондентите нямат създаден план за отговор на вътрешни заплахи. Респондентите на проучването са посочили, че незлонамерените вътрешни действия са причинили по-големи загуби на чувствителни данни, отколкото злонамерените действия отвътре (които са два пъти повече). В същото време сред предприетите действия за справяне със заплахите, по-голямата част заявяват, че решават проблемите вътре в самата организация, без да се стига до съд и правни последици.

През 2013 година 85% от организациите по света са се сблъскали с вътрешни инциденти, които в немалко ситуации са причинили загуба на поверителна информация, а за Източна Европа показателят е 87%, показва проучване на Global Corporate IT Security Risks 2013, проведено от изследователската компания B2B International съвместно с Лаборатория Касперский (Кръстева, Вътрешните заплахи за ИТ сигурността – масово явление, 2013).

Проучването откроява и трите най-често срещани вътрешни заплахи:

- уязвимости и грешки в програмното осигуряване;
- случайно изтичане на данни по вина на сътрудници;
- загуба или кражба на данни от мобилни устройства.

Джейсън Кларк - изследовател към центъра CERT при Института по софтуерно инженерство на университета Карнеги Мелън заключава, че „Преди всичко вътрешните нарушители могат да преодолеят съществуващите мерки за физическа и електронна защита чрез легитимни средства“ (CERT, n.d.).

За минимизиране на вътрешните рискове, свързани със сигурността, организациите прилагат различни мерки, в това число изолиране на критично важни мрежи - 57% и диференциране на правата за достъп до елементите на корпоративната ИТ инфраструктура - 51%, решения за контрол на мобилни устройства и за защитата им - само 28% или за криптиране на данните на системни носители - 36% сочат данните от проучването на Global Corporate IT Security Risks 2013.

Превантивните действия по отношение на вътрешните заплахи зависят от политиките на организацията и от степента на сигурност, наложена в мрежата. Като такива можем да посочим одит на вътрешния трафик и защитни стени с филтър (вж. глава 3, т.3.3.4). Според нас е препоръчително компаниите да се насочват и към програми за обучение, както и към външни възможности за наставничество (т.нар. коучинг) за развиване на вътрешните си сътрудници.

В заключение можем да обобщим, че заплахите за информационната сигурност непрекъснато се развиват и поставят нови предизвикателства пред ИТ специалистите.

Социалните мрежи могат да бъдат ценни продажбени и маркетингови инструменти. Макар, че са популярно средство за общуване, тези приложения крият множество рискове за сигурността, които могат да поставят потребителя или компанията в позиция на компрометиране или на сериозен риск.

Мобилните устройства от своя страна са сред основните предизвикателства през последните години. Организациите се опитват да се преборят с новите атаки, които злонамерени лица могат да извършат чрез мобилни компютърни устройства, собственост на работодател или служител.

Социалният инженеринг се очертава като много опасна техника за манипулиране на потребителите с цел придобиване на поверителна информация.

Вътрешните заплахи могат да се причислят към най-важните и сериозни заплахи пред ИТ сигурността на бизнеса, в които се включват неудовлетворени служители, непреднамерено изтичане на информация, неоторизиран достъп до данни и други.

Ограничаването на заплахите в дигиталното общество е неразривно свързано със създаването на правила и култура на поведение, които задължително да се спазват в неговите рамки. За осъществяването на тези дейности се изисква време и усилия не само от технологичен, но и от социален характер. Важно е да се разработи и предложи превантивна политика, която да отчита възможните заплахи, а обществото следва постоянно да бъде информирано за появата на нови хакерски заплахи, които непрекъснато ще се появяват заедно с технологическите усъвършенствания - задача както за експертите, така и за медиите.

1.3.4. Анализ и управление на риска в електронната търговия

1) Анализ на риска

Оценката на риска е основен етап в процеса на формиране на политика за сигурност, която да отчита специфичните особености и да снижава риска до приемливо ниво при осъществяването на електронни транзакции. Стъпките на този процесен етап се повтарят циклично до получаване на пълна и ясна картина за рисковете, които застрашават електронните транзакции на компанията. Оценката на риска решава въпроса за резултатите, които трябва да се постигнат при имплементирането на политиката за сигурност. Като самостоятелен процес, оценката на риска включва девет стъпки, които включват: характеристика на системата; определяне на заплахата; идентифициране на уязвимостта; контролен анализ; определяне на вероятност дадено събитие-заплаха да се случи; анализ на въздействието; определяне на риска; препоръки за контрол; документация на резултатите (Илиев, 2012).

Съществуването на риск при осъществяването на онлайн търговията налага необходимостта да се разреши на експертите по защитата и системните администратори да определят за кои рискове е наложително да се проектира защита и за кои не е необходимо. Този процес се нарича **анализ на риска**.

Най-общо анализът на риска може да се дефинира като процес, при който се изследват заплахите и слабите места за СЕТ (Hightechbg.com, n.d.). Целта на този процес е рисковете да се подредят и на базата на възможните щети от реализацията на тези рискове, да бъдат оправдани направени вече или планирани разходи за сигурност.

На най-високо равнище анализът на риска включва три фази:

- Дефиниране на стойност на ресурсите, при което се използват различни подходи. Някои от тях прилагат традиционни, а други по-комплексни измерители, които трябва да бъдат отчетени при определянето на стойността на даден ресурс.

- Присвояване на стойност на рисковете – използва се показателят **очакване за единична загуба (single loss expectancy - SLE)**, чрез който с помощта на сравнения се определя какви ще бъдат щетите за ресурс при проявлението на даден риск (Landoll, 2011). Изчисляването само на очакването за единична загуба не е достатъчно, за да се вземат решения по отношение на риска. Също така е необходимо да се отчете честотата на поява на риска, както и най-малката вероятност за това.

- Избор на мерки за противодействие – изборът се прави, в зависимост от множество изчисления и анализи относно честотата на проява на даден риск, както и стойността на евентуалните щети след настъпването му. Съществува възможност разходите за редуциране на риска до необходимото равнище да са по-високи от стойността на ресурса, който трябва да бъде защитен (Стоилов, Уязвимост на системите при свързване на корпоративните мрежи с мрежите за управление на технологични процеси, 2010).

Въпреки че чрез анализа на риска се стреми да се открие разумен начин за редуцирането му с предприемане на мерки за противодействие, то в някои случаи по-интелигентният подход би бил да се прехвърли отговорността върху друго лице или организация, или просто да се поеме този риск.

Задълбоченият анализ на риска преследва две цели:

- подпомага ИТ специалистите да вземат верни решения относно сигурността;
- може да се използва като средство за удостоверяване на коректност относно предприети действия по отношение на информационната сигурност.

В зависимост от начина, по който се осъществява, анализът на риска може да бъде (Стоилов, Управление на мрежовата сигурност. Системи за откриване на нарушители, 2011):

- **количествен анализ**, при който на всеки ресурс се дава стойност в количествено изражение и тази стойност се съпоставя с разхода за противодействие на свързаната с ресурса заплаха;
- **качествен анализ**, който използва компетентността на служителите, които са запознати с организацията в най-голяма степен.

Разгледаните подходи имат своите предимства и недостатъци. При разработването на решение за сигурност подходите трябва да бъдат разглеждани като взаимно допълващи се, тъй като за да се извърши ефективна оценка на риска, е необходимо да се приложат и двата подхода.

След анализа на рисковете и определянето на потенциалните загуби от проявлението им, може да започне процесът по **управление на риска**.

Управлението на риска е комплексен процес, който включва (Стоилов, Управление на мрежовата сигурност. Системи за откриване на нарушители, 2011):

- **определяне** на едно приемливо ниво на риск;
- **оценяване** на текущите нива на риска;
- **приемане** на стъпки за намаляване на риска до определеното вече приемливо ниво;
- **поддържане** на това ниво.

Управлението на риска започва със съставяне на **списък на рисковете** за системата. Списъкът на рисковете е съставен от рискове, които могат да бъдат определени **количествено**. Това най-добре може да бъде направено на работна среща на всички заинтересовани страни от един или друг ресурс – компонент на СЕТ.

Необходимите части, които трябва да съдържа списъкът с рисковете включват:

- **име на ресурса** - компонентът, който трябва да бъде защитен. В СЕТ типичните ресурси, които се използват са уеб сървър, сайт на електронния магазин, мрежа, клиентски данни и др. (вж. глава 3, т. 3.3.2.)
- **уязвимост** - слабост, физическо излагане или излагане на процес, които правят ресурса податлив на неправомерно използване. В процеса на ЕТ като уязвимости можем да посочим слабости в кода както на сайта, така и на приложенията за ЕТ, слаби пароли и др.
- **възползване** - използване на една или повече уязвимости, за да се атакува ресурса. Като най-често срещани възползвания можем да посочим подслушване на мрежата, атаки към клиентските компютри и сървърите и др.;
- **вероятност** - оценяване на вероятността възползването да се случи;
- **въздействие** - тежестта на повредите, когато някой се възползва от уязвимостта.

Следователно, **Риск = Вероятност * Въздействие** (1)

Редуцирането на рисковете може да се извърши чрез предприемането на различни **контрамерки**, които се проектират и прилагат на основа на установената **тежест на рисковете** в списъка на рисковете.

Определянето на разходите за информационна сигурност по отношение на рисковете включва следните стъпки:

- оценяване стойността на информационните ресурси;
- изреждане на рисковете, които се отнасят за тези ресурси и стойността, която трябва да се заплати, в случай че рисковете се реализират;
- подбор на мерки за превенция на база ефикасност и разходи за изпълнението им, съпоставени със стойността на риска.

Разработени са множество **техники** за контролиране на рисковете. Някои от тях включват:

- **поемане на риска** – рискът може да бъде поет, ако вероятността да се случи е много малка, разходите за щетите, нанесени от реализиране на риска са ниски, а разходите за смекчаване на риска са високи;
- **избягване на риска** – не се допускат действия, които излагат ресурсите на риск;
- **прехвърляне (трансфер) на риска** – прехвърляне на риска към застрахователна компания;
- **смекчаване на риска** – предприемане на процедури по елиминиране на риска. Част от методите за смекчаване се свеждат до:
 - **проектиране за минимален риск** - проектиране на системата с цел елиминиране на възможно повече рискове;
 - **включване на защитни устройства** - намаляване на риска чрез използване на устройства като защитни стени и преграждащи рутери. Тези устройства обикновено не влияят на вероятността, но намаляват тежестта на експлоатация;
 - **осигуряване на предупреждаващи устройства**. Предупреждаващите устройства могат да бъдат използвани, за откриване на нежелано състояние и алармиране на персонала. Пример е системата за откриване на проникване (Intrusion Detection System - IDS), която сигнализира системния мениджър, в случай, че системата е подложена на атака.
 - **разработване на процедури и обучение**. Обучението и процедурите могат да смекчат рисковете, които са свързани със самите хора (социален инженеринг и др.).

Можем да обобщим, че анализът на риска е процес, при който се установяват заплахите и уязвимите места на електронните магазини или комуникационните връзки към тях, вероятността за осъществяване на заплахите при конкретните ресурси и работна среда и се оценяват последствията при тяхното реализиране. Основните рискове в СЕТ включват хакерски атаки и кражба на информация, манипулиране на клиенти, злоупотреби с банкови карти и др. За да се гарантира безопасността на информацията в СЕТ, трябва да се изберат такива мерки за сигурност, включително застраховка, каквито са необходими за контролиране на риска в допустимите граници на най-ниска цена. Тези мерки се определят на база съотношението цена/сигурност, които те осигуряват. Това от своя страна изисква количествена и качествена оценка на потенциалните ползи от всяка мярка за сигурност в СЕТ.

2) Методи за количествен и качествен анализ на риска

Количествен анализ на риска

Процесът започва с набирането на данни за ресурсите на бизнес организацията, като за всеки от тях се дефинира стойност, която включва разходите за подмяна на ресурса, стойността му за конкурентите, значимостта му за рентабилността на компанията и т.н.

Раздробяването на ресурса на отделни части при определянето на стойността му, предоставя възможност за по-прецизен избор. При разделянето не трябва да се стига до крайност, понеже анализът може да се затрудни.

Следващата стъпка е съставянето на списък с рисковете за всеки ресурс, които са обвързани с понасяне на евентуални загуби, ако конкретният риск се реализира. Всеки риск се характеризира с понятието **очакване за единична загуба (single loss expectancy – SLE)**. Неговото изясняване въвежда понятието **фактор на очаквана загуба (Exposure Factor – EF)** (Stewart, 2012). Това е субективно, потенциално поражение на определен ресурс, което се изразява в процент и е резултат от реализирането на отделна заплаха (Стоилов, Управление на мрежовата сигурност. Системи за откриване на нарушители, 2011).

За определяне на SLE се използва следната формула:

$$\text{SLE} = \text{Стойност на ресурса} \times \text{EF} \quad (2)$$

След като SLE е изчислено, заплахата може да бъде анализирана. По своята същност тя може да бъде с човешки, природен или технически характер. Това, което трябва да се определи, е колко често се очаква компанията да бъде подложена на конкретна заплаха като се има предвид, че не са предприети мерки за превенция. Описаният индикатор се нарича **годишна честота на реализация на риска (Annualized rate of occurrence - ARO)** (Gibson, 2011). Стойностите на показателя варират, в зависимост от проявлението на дадена заплаха. Ако индикатора е със стойност 1, заплахата ще се прояви поне веднъж в годината, а ако е равен на 0, то няма вероятност бизнес организацията няма да се сблъска с тази заплаха. Тези стойности ни дават основание на направим извода, че даден риск може да се реализира повече от веднъж годишно (Gibson, 2011).

Изчисляването на ARO се извършва посредством беседи с експерти, като за специфични заплахи показателят може да приема различни стойности.

Свързването на годишната честота на реализация на риска с очакването за единична загуба, позволява изчисляването на показателя **очаквана годишна загуба (Annualized loss expectancy - ALE)**. Очакваната годишна загуба е правопропорционална на SLE и ARO, т.е.:

$$\text{ALE} = \text{SLE} \times \text{ARO} \quad (3)$$

Най-същественният недостатък на количествения анализ е в това, че въпреки неговата коректност, е много трудно да бъде реализиран правилно. Обикновено становищата на разработващите оборудване и на анализаторите на риска се разминават по отношение на типове заплахи и честотата на появяването им. Освен това, резултатите от този анализ могат да се окажат само една експертна хипотеза, ако зад тях няма сериозно количество събрани и анализирани автентични данни. Сериозен недостатък също представлява фактът, че процесът на натрупване на данни е значително труден и методологически недостатъчно изяснен.

По тези причини в много от случаите компаниите и специалистите по сигурността се насочват към различен метод за оценка на риска, а именно качественият анализ.

Качествен анализ на риска

Този подход на анализ разчита на знанията и уменията на служителите, които са най-добре запознати с ресурсите на компанията, като компетенциите им ще се използват,

за да се определят рисковете за ресурсите и съответно избор на мерки за превенция. Процесът на събиране на информация от експертите се нарича „Делфи техника“ (**Delphi Technique**) (Kim, 2012) .

Подходът на качествения анализ е сходен с този на количествения анализ, с тази разлика, че тук не се използват числа и формули.

Тъй като качественият анализ в известна степен се базира на субективна оценка, то той е по-ефикасен, когато в него вземат участие по-голям брой специалисти. При прилагането му може да се използват множество техники, като въпросници с оценки, интервюта, съвещания, цялостни хипотетични въпроси, които да позволяват на експертите да формулират становищата си относно заплахите и редуцирането на рисковете. Практиката налага всяко мнение във връзка с рисковете за организацията да бъде изследвано, тъй като това е в полза на качествения анализ на риска. Безспорно е, че група от експерти може да идентифицира повече рискове и да предложи по-широк спектър от ефективни механизми за превенция, отколкото един единствен аспект.

Главно предимство на качествения анализ е, че той е гъвкав и лек за изпълнение и изчисленията, които използва не са сложни, но той има и редица несъвършенства. Съществен недостатък при него се дължи на субективната същност на анализа и отсъствието на обективни данни относно стойността на ресурсите. Резултатите от него могат да варират в доста широк диапазон, в зависимост от надценяването или подценяването на действителната стойност на ресурса. Въпреки това съществуват случаи, в които точно този проблем допринася за популяризирането на качествения анализ.

Основни методи, използвани при качествения анализ на риска

За реализиране на качествения анализ са прилагани различни методи. Най-често използваните от тях са:

- експертни оценки;
- списъци и въпросници за идентификация на рискове;
- диаграма „Рибена кост“;
- писане и анализ на сценарии;
- сравнение с аналози и систематизиране на добри практики;
- матрица „Критичност на ресурсите – последствия“;
- модел за анализ на йерархии.

Нека направим кратък анализ на тези методи.

Експертни оценки

Методът представлява съвкупност от знания и целенасоченото им използване за реализиране на методиката, принципите и изискванията за реалното и ефективно оценяване на защитаваните обекти в СЕТ, които включват електронен магазин, сървър и др. (Шишманов К. К., 2007).

Основната цел на експертните оценки е да се проследи пътят на практическото използване на експертните знания и по този начин най-рационално да се използва човешкият фактор в процеса на образуването на експертните оценки.

Най-съществените предимства на метода се свеждат до гарантиране високото качество на оценката, която не се влияе от външни или субективни фактори; получаване на резултати, които могат да се използват в други направления; обединяване и обмяна на знания с други експерти, занимаващи се с проблематиката.

Експертните оценки имат някои слабости, които не позволяват прилагането им в определени случаи. Такива слабости са частична автоматизация; ограничен обхват на предметната област; липса на комплексна оценка и обвързаност с други методи.

Списъци и въпросници за идентификация на рискове

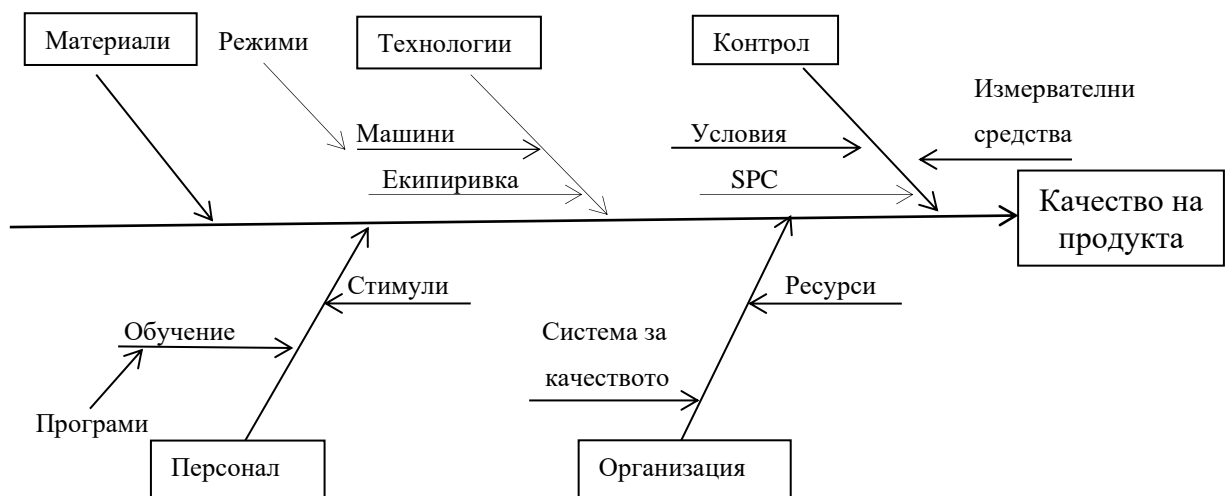
Списъците с рискове представляват таблици, в които са дефинирани рисковите области в СЕТ и съответстващите им рискове. Те се обогатяват и доразвиват със събирането на данни и информация при функционирането на бизнес организацията, както и с добавянето на въпросници, съпроводени с отговори.

Информацията в списъците може да бъде извличана от най-различни източници, като такива могат да бъдат отчети за вече изпълнени успешни и неуспешни проекти, планове за управление на рисковете от минали периоди, систематизирани резултати от анализи на добри практики, научни публикации, публикации на браншови организации и натрупан опит на заинтересовани от функционирането на организацията лица.

Диаграма „рибена кост“ (диаграма на Ишикава)

Този метод се базира на експертни мнения относно първоизточниците за настъпване на определен ефект (Hannagan, 2008). Специалистите проучват всички рискови зони в СЕТ, с цел уточняване на всички възможни причини за ефекта, като причините могат да се поставят на различни логически нива. Това най-често се постига с метода на мозъчната атака, като целта е да се извърши систематизиране на възможните причини за реализиране на разглеждания риск.

С подробното описване на всички рискове в СЕТ се формира графичен модел на рисковете за дадена бизнес организация, групирани по определени признаци, наречен карта на рисковете. Разработеният модел дава възможност за визуално изобразяване на групите рискове, характерни за организацията, а също и връзките между тях.



Фиг. 1.6. Диаграма „Рибена кост“ (диаграма на Ишикава), източник: (Дюкенджиев, 2008)

Съставяне и анализ на сценарии

При този метод се съставят сценарии на евентуално проявление на рисковете в СЕТ. Тези сценарии не се стесняват до прогноза на предстоящо състояние на рисковете за бизнес организацията, а описват пътя и начина за достигане на това състояние.

Информацията, на чиято база се създават сценарии, може да бъде с най-различен произход. Обикновено се използват експерти в областта на ЕТ; висши мениджъри в организацията; публикувана информация за съществени тенденции и настъпване на събития, които могат да повлияят; външна среда на организацията (икономическа, технологична, социална); стратегически действия, които участниците могат да предприемат.

Сравнение с аналози и систематизиране на добри практики

Целта на този метод е да се направи връзка между идентифицирани реално реализирани се рискове при функционирането на СЕТ. Методът се прилага при условие, че подобни анализи са се извършвали в миналото, или бизнес организацията разполага с информация от анализи в други компании. Тези анализи могат да бъдат солиден източник на информация – основа за анализ на риска.

Матрица Критичност на ресурсите – последствия

Този модел цели да се оценят разработваните и използваните при функционирането на СЕТ ресурси, относно критичността им и последиците, ако те бъдат повредени или унищожени.

Критичността на ресурса се оценява по важността му за постигането на целите на бизнес организацията, като тя може да бъде вътрешна и деривативна. Вътрешната критичност се дефинира според значимостта на ресурса за изпълнението на целите на организацията, а деривативната се оценява според щетите, които евентуално ще бъдат понесени при загуба на съответния ресурс.

Модел за анализ на йерархии

Този метод дефинира систематична процедура за представяне на съставните части на един проблем в СЕТ в йерархичен вид. Според методологията, първо проблемът постепенно се разделя на своите съставлящи елементи, а след това се предоставя възможност, на основата на серия сравнения между тях, да се представи силата на влиянието им в йерархията.

Методът може да се използва за систематизиране на рисковете по приоритет, като се отчита вероятността за настъпване на дадено събитие и размерът на щетите, ако то възникне, както и за изчисляване на силата на влияние на всеки фактор върху относителния приоритет на съответния риск, а също и за оценка и избор на стратегии за управление на риска.

Комбиниране на количествения и качествения анализ на риска

В зависимост от организационната структура, управлението на организацията може да бъде удовлетворено от резултатите, получени от качествения анализ. За да бъдат оправдани разходите за сигурност, извършени от една организация, са необходими конкретни данни и информация, които се използват при количествения анализ. Практиката показва, че се използват елементи и от двата вида анализ.

При изчисляването на показателите в количествения анализ често се използват похвати на качествения подход. Броят на организациите, които са в състояние авторитетно да прогнозира конкретни стойности за индикаторите в количествения анализ, е значително малък. Тези показатели се изчисляват по-коректно при дискусия със специалистите, чиито мнения произхождат от собствената им интуиция и опит (Стоилов, Управление на мрежовата сигурност. Системи за откриване на нарушители, 2011).

В заключение можем да отбележим, че двата подхода за анализ на риска имат своите предимства и недостатъци и използването им е задължително в процеса на изграждане на информационната сигурност на организацията. Важно е да се подчертае, че не всички разгледани методи на двата подхода могат да бъдат имплементирани за дадена компания. За да се определи кои методи са необходими и подходящи за дадена организация, трябва да се извърши анализ на разходите и изгодите, който да установи, че разходите за реализиране на даден метод са оправдани с постиганото намаляване на нивото на риска. В допълнение можем да констатираме, че е необходимо задълбочено оценяване на оперативните последици на представените препоръки.

Основни изводи:

1. Електронната търговия е обект на множество изследвания. Съществуващите дефиниции я представят от различни гледни точки. Обобщавайки ги и като изхождаме от целите на настоящето научно изследване смятаме, че ЕТ може да бъде разглеждана като съвкупност от комерсиални транзакции, осъществявани и/или управлявани чрез електронни средства. Заедно с купувача и продавача, основни участници в тези транзакции са системите за: реализиране на електронен магазин, електронно заплащане, електронно фактуриране и др.

2. Транзакциите в електронната търговия са свързани с множество реални и потенциални рискове за сигурността, които трябва да бъдат изследвани, оценявани и ефективно да им бъде противодействано.

3. Информационната сигурност в системите за електронна търговия изисква осигуряване и поддържане на конфиденциалност, интегритет и достъпност на данните. Необходимо е ключовите компоненти на информационната сигурност да се анализират спрямо трите основни елемента на компютърните системи - хардуер, софтуер и средства за комуникация. Това се прави с цел разработване и имплементиране на стандарти за информационна сигурност като инструменти за защита и превенция на три нива - физическо, персонално и организационно. Развитието на нови направления на електронната търговия, като мобилна търговия, изисква разработването и следването на специфични правила и процедури, насочени към природата на мобилните устройства и имащи за цел тяхното контролирано използване, съгласно приетите политики и стратегии за сигурност.

4. Анализът на електронната комерсиална транзакция показва три потенциални ключови точки на уязвимост – съобщителните канали, сървърът и клиентът. Нормалното протичане на транзакциите ще зависи от поддържането на определено ниво на сигурност за всяка от тях. Повишаването на сигурността в тези точки се реализира с помощта на множество технологии като протоколи за сигурност, антивирусен софтуер, организационни процедури и др.

5. Основните заплахи за електронната търговия включват вредителски код, потенциално нежелани програми, фишинг и др., а основните тенденции в заплахите за ЕТ са насочени към социалните мрежи и Web 2.0 услугите, мобилните устройства, социалния инженеринг и вътрешните заплахи.

6. Поддържането на информационната сигурност в една система за електронна търговия е комплексен процес, който включва идентифициране на всички точки на уязвимост в системата и прилагане на адекватни защитни механизми за повишаване нивото на сигурност в слабите места.

7. Анализът на риска е основен етап от изграждането на информационна сигурност в системите за електронна търговия. Коректно извършеният анализ позволява да се премине към управление на риска, при който се предприемат стъпки за редуцирането му до едно приемливо за конкретната организация ниво.

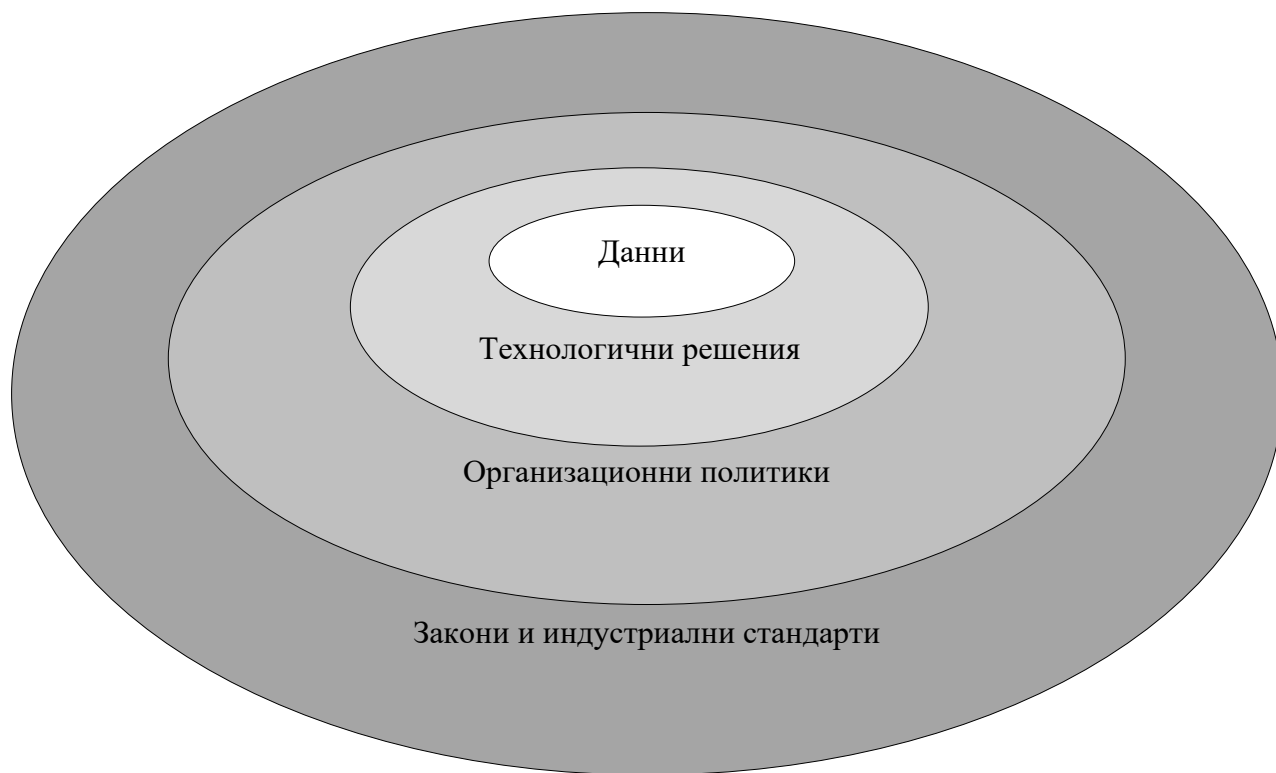
8. Основните технологични аспекти на защитата в ЕТ включват: защита и използваемост на системата за електронна търговия, потребителски имена и пароли за достъп, потребителски интерфейс, защита и мащабируемост, защита на електронните транзакции и дефиниране на минимално ниво за информационна сигурност.

Втора глава. Технологии и стандарти, поддържащи защитена среда за функциониране на електронната търговия

2.1. Компоненти на защитената среда за електронна търговия

Проблемите за сигурността в ЕТ са сериозни и многоаспектни. Тяхното решаване се нуждае от последователна стратегия и политика, които се базират на съвременни бизнес модели.

Подходящ модел, който ще използваме за защита на СЕТ, е представен от Лоудън и Тревър (Laudon К. Т., 2013). Според тях резултатната защита в онлайн търговията е многопластова и тя трябва да отчита новите технологии, политики и процедури, закони и индустриални стандарти, за да се осигури висока степен на защитата за хората и организациите в ЕТ.



Фиг. 2.1. Модел за ефективна защита на данните в ЕТ, източник: (Laudon К. Т., 2013)

Преди да анализираме моделът на Лоудън и Тревър за поддържане на защитена среда за ЕТ, трябва да обърнем внимание на три своеобразни противоречия (конфликта), касаещи директно или индиректно всеки един модел и стратегия за защита и особено защита в ЕТ.

На първо място това е вечният конфликт между увеличаване на инвестициите, необходими за поддържане на защитата от една страна, а от друга, идеята за снижаване на общите разходи. Компютърната защита увеличава разходите за бизнес операции и за складиране на данни. Тя е разход, който може да намали общата стойност на бизнеса. Прекалено строгата защита може да намали печалбата, докато слабата защита – да провали бизнеса. От тук следва и изискването за много прецизно „дозиране“ на разходите за

защитни механизми, което усложнява изключително много работата по разработването на моделите за защита.

Второто противоречие е свързано с факта, че повече защитни механизми, които са добавяни към сайта за ЕТ, засилват сигурността му. От друга страна те усложняват неговото използване и по този начин затрудняват част от потребителите.

На трето място, трябва да споменем противоречието между желанието на хората да действат анонимно (да крият идентичността си) и необходимостта от автентификация, за да се противодейства на престъпници или злонамерени лица.

Смятаме, че на тези противоречия може да се реагира единствено чрез компромиси в един или друг аспект и постоянно да се следи развитието на технологичните решения, които могат да им повлияят.

2.1.1. Измерения на информационната сигурност в електронните транзакции

Моделът на Лоудън и Тревър се базира на шестте измерения на защитените транзакции в ЕТ, които са: *интегритет (цялостност), неотричане, автентификация, конфиденциалност, неприкосновеност на личните данни и достъпност*.

Таблица 2.1. представя тези измерения в два аспекта: от гледна точка на клиента и от гледна точка на търговеца (Laudon K. C., 2013).

Таблица 2.1.

Измерения на информационната сигурност

Измерение	Перспектива на клиента	Перспектива на търговеца
Интегритет	Променя ли се предаваната или получаваната информация	Валидна ли е предаваната от клиента информация
Неотричане	Възможно ли е да не се изпълнят поети дейности	Може ли клиентът да откаже поръчката
Автентификация	Сигурно ли е, че срещнатата страна е тази, за която се представя	Сигурно ли е, че срещнатата страна е тази, за която се представя
Конфиденциалност	Възможно ли е външно лице да прихваща и прочита съобщенията	Възможно ли е външно лице да прихваща и прочита съобщенията
Неприкосновеност на личните данни	Може ли клиентът да контролира използването на предаваната информация	Използва ли се предоставената информация от клиентите неправомерно
Достъпност	Достъпен ли е сайтът	Функциониращ ли е сайтът

Моделът оформя две групи решения: технологични решения и политически решения. Защитата в ЕТ се проектира така, че да защитава посочените по-горе шест измерения. Компромис, с което и да е от тях би породил сериозни проблеми за защитата.

2.1.2. Технологични решения за информационна сигурност в електронната търговия

Електронните транзакции се извършват през глобалната мрежа Интернет и данните за тях преминават през множество маршрутизатори и сървъри, поради което експертите по сигурността смятат, че най-големите заплахи идват точно от Интернет комуникациите.

За защита на Интернет комуникациите се използват множество инструменти като криптиране, защитени канали за комуникация, защитени мрежи, защитени сървъри и клиенти (Laudon К. Т., 2013).

А. Криптиране

Криптографията е основната методология, която осигурява възможност за създаване на механизмите за удостоверяване, цялост и конфиденциалност.

Осигуряването на удостоверяване, цялост и конфиденциалност се осъществява от четири функции:

- симетрично криптиране с ключ;
- асиметрично криптиране с ключ;
- еднопосочни хеш функции;
- цифрови подписи.

За целите на изследванието ние смятаме, че е необходимо тези функции да бъдат разгледани и анализирани по-подробно.

Симетричното криптиране, познато още като криптиране с таен ключ, използва един и същи ключ и криптографски алгоритъм, за да шифрира и дешифрира съобщенията.

Съществуват специфични алгоритми с таен ключ, които обработват отделни фрагменти от съобщението с фиксирана дължина, поради което е нужно обемните съобщения да се разделят на произволни блокове и след това да се обединят (Pachghare, 2009). Механизмите за свързване добавят допълнителна защита срещу прихващане на предаваните данни.

На разположение са четири разпространени режима, които определят метод за комбиниране на некриптираното съобщение, таен ключ и криптиран текст, за да се получи поток от шифриран текст, предаван към получателя (Yen, 2006):

- Electronic CodeBook (ECB);
- Cipher Block Chaining (CBC);
- Cipher feedback (CFB);
- Output FeedBack (OFB).

Механизмът ECB кодира независимо всеки блок и използва един и същ ключ, докато останалите три алгоритъма (CBC, CFB и OFB) съдържат свойства на непостоянност, които добавят елемент на случайност към криптираните съобщения.

Някои от по-често използваните алгоритми с таен ключ днес са (James, 2008):

- Data Encryption Standard (DES);
- 3DES (троен DES);
- Rivest Cipher 5 (RC5);
- International Data Encryption Algorithm (IDEA);
- Advanced Encryption Standard (AES);
- Blowfish;
- Twofish;
- Carlisle Adams/Stafford Tavares (CAST 128).

Симетричното криптиране можем да използваме в СЕТ за защитена комуникация между клиента и сайта на електронния магазин, както и между клиента и системите за електронни разплащания (вж. глава 3, т.3.3.4).

Асиметрично криптиране

Асиметричното криптиране е известно като криптиране с **публичен ключ** и ползва един и същ алгоритъм или различни, допълващи се алгоритми за шифриране и дешифриране на данните. Необходими са две различни стойности за ключове - публичен ключ и частен ключ (Andress, 2011). Публичният ключ се използва за криптиране на данни от изпращащия към получаващия, а частният ключ - за декриптиране на изпратеното съобщение.

Поради ограниченията си по отношение на производителност, алгоритмите за криптиране с публични ключове рядко се ползват за гарантиране конфиденциалността на данните. Приложението им е насочено за процеси, които включват удостоверяване посредством електронни подписи и управление на ключове. Известни алгоритми с публични ключове включват алгоритъм на Рон Ривест, Ади Шамир и Леонард Аделман (RSA) и алгоритъм на Ел Гамал, PGP.

Хеш функции

Хеш функцията е изчислително ефективна функция, преобразуваща двоична последователност с променлива дължина в двоична последователност с фиксирана дължина (Буюклиева, 2007). Резултатът с фиксирана дължина от функцията се нарича **хеш**, или представител на съобщението. Алгоритмите, които могат да бъдат определени като сигурни с хеш, трябва да притежават следните свойства (Каео, 2006):

- функцията трябва да бъде постоянна, т. е, един и същ аргумент трябва винаги да води до един и същ резултат;
- функцията трябва да бъде еднопосочна (необратима) – вижда се резултатът, но е изключително трудно да се установи входящото съобщение;
- резултатът от функцията трябва да бъде случаен или да създава впечатление за случайност, за да се предотврати възстановяване на началното съобщение;
- резултатът на функцията трябва да бъде уникален;
- трябва да е почти невъзможно да се открият две съобщения, водещи до един и същ представител на съобщението.

Хеш функциите са няколко вида:

- Modification detection code (MDC) – те не използват таен ключ и се използват само за проверяване на интегритета на данните;
- Message authentication code (MAC) – те използват таен ключ извършват удостоверяване на източника на информацията.

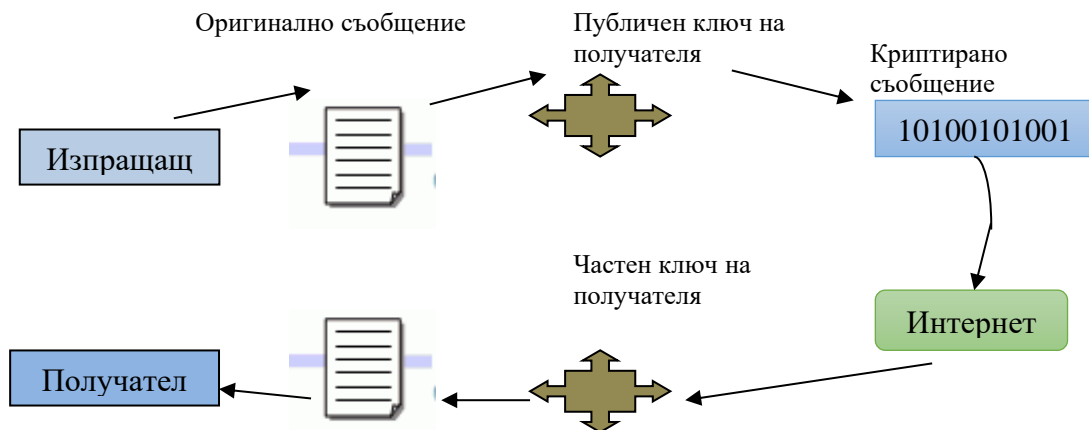
Най-често срещаните алгоритми за хеш функции са следните:

- Алгоритъмът Message digest 4 (MD4);
- Алгоритъмът Message digest 5 (MD5);
- Secure Hash Algorithm (SHA).

В СЕТ асиметрично криптиране и хеш функциите може да се използват за получаване на електронен подпис, който осигурява защита на комуникациите между системите за електронни разплащания и страните на електронните транзакции (вж. глава 3, т.3.3.4).

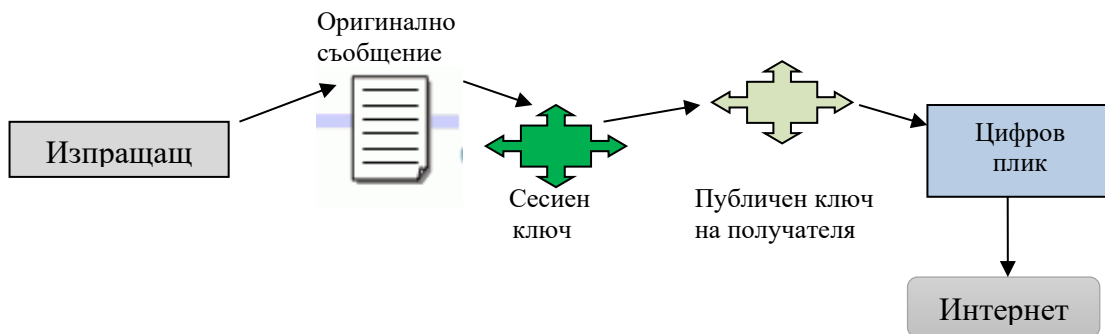
Технологията на **електронния подпис** в голяма степен дава решение на проблемите със сигурността на пренасяната информация (Орсов, 2001). Той представлява криптографски подпис, който се получава при шифриране на информацията, направено с цел да се удостовери изпращащият и да се даде гаранция, че информацията не се променя по пътя между изпращането и получаването (Searchsecurity, n.d.). Цифровите подписи се базират на комбинация от криптиране с публичен ключ и от еднопосочни защитени алгоритми с хеш функции. Най-използваните алгоритми за цифров подпис с публичен ключ са RSA, Digital Signature Standard (DSS).

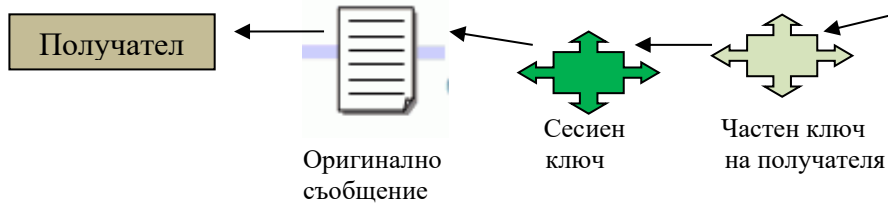
В практиката се използват три разновидности на електронния подпис - обикновен електронен подпис, усъвършенстван електронен подпис и универсален електронен подпис.



Фигура 2.2. Криптиране с публичен ключ, използвайки цифров подпис и хеш, източник: (Privatesky, 2014)

Съществуват случаи, в които се изисква индивидуално криптиране на отделно съобщение с таен ключ. При такъв случай изпращащият и получаващият съобщението си разменят тайния ключ за криптиране и съответно декриптиране, при което съществува риск от прихващането му. Криптирането с публичен ключ предлага ефективно решаване на този проблем с въвеждането на технология, наречена *цифров плик* (Newman R. С., 2010). Цифровият плик се състои от криптирано с таен ключ съобщение, заедно с криптирания таен ключ с техниката на публичното криптиране. При установен таен ключ от изпращача и получателя, той може да бъде използван за декриптиране на тайния ключ от цифровия плик. Тази техника може да бъде използвана за криптиране на отделно съобщение или на разширена комуникация.





Фиг. 2.3. Криптиране с публичен ключ, използвайки цифров плик,
 източник: (Slideshare.net, 2014)

Проблемите при размяна на ключове за криптиране също така могат да се решат и с използването на технологията на *цифровите сертификати*, която установява връзка между даден потребител и неговия публичен ключ (Kahate, 2013). Следователно цифровият сертификат трябва да съдържа имената на даден потребител и потребителския публичен ключ, с което да се гарантира, че даден публичен ключ принадлежи на точно определен потребител.



Фиг. 2.4. Цифрови сертификати и сертифициращи органи
 източник: (Laudon К. Т., 2013)

Доставчиците на удостоверителни услуги в България са Информационно обслужване АД, Борика Банксервиз АД, Инфонотари АД, Спектър АД и СЕП България АД (CRC.bg, n.d.).

Наред с безспорните предимства, криптографските методи имат редица **недостатъци**, които трябва да се вземат предвид при разработване и избор на оптимално приложение. При **симетричните системи** тайният ключ е само един и може да бъде компрометиран съзнателно или целенасочено. Също така ключът трябва да се заменя при всяка сесия, което довежда до проблеми с разпространението на ключове. На последно място, симетричните системи не са подходящи за електронен подпис, понеже изискват дълги ключове за проверка и замесване на трета доверена страна. По отношение на **асиметричните системи** за криптиране - те са по-бавни от симетричните, ключът е по-дълъг от

този на симетричните и добавеният електронен подпис е със сравнително голяма дължина.

Можем да обобщим, че системите на криптиране осигуряват четири от основните шест измерения на информационната сигурност в СЕТ, които са интегритет, автентификация, неотричане и конфиденциалност. Приложението им за защитена комуникация и електронно подписване гарантират безрисковото функциониране на процесите в ЕТ.

Б. Защитени канали за комуникация

Защитените канали за комуникация се реализират основно чрез протоколите Secure Sockets Layer (SSL) и Transport Layer Security (TLS), както и комбинация от тях и осигуряват сигурен обмен на информация между потребителите.

За осигуряване на сигурност на транзакциите се използва **SSL** - протокол за връзка между браузъра на клиента и сървъра, при която се гарантира неприкосновеност, интегритет и мерки за автентификация за предотвратяване на несигурни мрежови връзки (Davies, 2011).

Протоколът TLS се използва в комбинация с SSL и чрез него клиентски/сървърни приложения имат възможност да комуникират в мрежата, без да съществува риск от подслушване и модифициране. TLS клиентът и сървърът договарят динамична връзка чрез процедура на „ръкостискане“ (handshaking), където се установява съгласие по различни критерии, които се използват за да се установи криптираната връзка.

Протоколите SSL и TLS намират приложение за защита на комуникациите между клиентите и електронния магазин, както и между системите за електронни разплащания и страните на електронната транзакция (вж. глава 3, т.3.3.4)

Виртуални частни мрежи VPN

Виртуалните частни мрежи се използват за установяване на сигурни лични мрежови връзки от точка до точка като се използва инфраструктурата на публична мрежа чрез т. нар. „тунелиране“ (Каео, 2006). Много бизнес организации създават частни и доверени мрежови инфраструктури, като използват вътрешни или външни кабелни съоръжения и широкомащабни мрежи, за да предложат ниво на конфиденциалност въз основа на физическа защита. Като форма за пренос на данни, виртуалните частни мрежи могат да редуцират значително рисковете за сигурността от използването на Интернет, измествайки по-скъпите наети линии. От гледна точка на потребителя, естеството на физическата мрежа, която се тунелира, не е от значение, защото изпращането на информацията е сходно с изпращането по частна мрежа.

Виртуалните частни мрежи намират приложение в предложени архитектурен модел за СЕТ основно при комуникациите в отношенията бизнес към бизнес (вж. глава 3, т.3.3.4).

В. Защитени мрежи

Една от техниките за осигуряване на солидна защита от външни атаки е чрез изолиране мрежата от Интернет. Изолирането на мрежата основно се реализира с използването на прокси сървър и защитна стена.

Прокси сървърът (сървърът-посредник) е компютърна система или набор от програми, които функционират като посредник за търсените от потребителите услуги от други сървъри (Chou, 2012). Потребителят установява връзка с прокси сървър, като изисква конкретни услуги, достъпни от друг сървър, след това прокси сървърът извършва проверка на заявката, в съответствие с дефинирани правила за филтриране. Ако искането бъде потвърдено, прокси сървърът предоставя исканата услуга, чрез установяване на

връзка със сървъра, който действително предоставя услугата и изисква услугата от името на клиента.

Прокси сървърите се използват с различни цели:

- опазване анонимността на машините, които използват услугата, главно с цел сигурност;
- увеличаване на скоростта на достъп до ресурси чрез кеширане;
- реализиране на процедури за достъп до мрежи, блокиране на нежелани сайтове;
- следене и анализ на потребление на дадени ресурси от служителите на дадена организация;
- заобикаляне на приложени разпоредби за сигурност, като родителски контрол и др.;
- проверка на данни срещу зловреден софтуер преди получаването им от потребителя;
- сканиране на изходящи данни, в случай че изтичат незащитени данни.

В решението за информационна сигурност за СЕТ, което предлагаме в глава 3, т.3.3.4, прокси-сървърът може да се използва в мрежата на бизнес организацията за защитена връзка между клиента и вътрешната мрежа на търговеца. Прокси-сървъри се ползват предимно от бизнес организации от среден и голям размер.

Защитна стена (Firewall)

Защитна стена или Firewall представлява защитен механизъм, който може да се реализира по многобройни начини (Steward, 2010). Идеята ѝ е да осигури на локалните потребители достъп до всички услуги на мрежата, а също и някои уеб услуги, като заедно с това да контролира обмена на данни и външния достъп до локалните ресурси. Защитната стена реализира сигурност, като изолира локалната мрежа от външните мрежи. Трафикът трябва да се контролира по начин, който гарантира засичане на всички видове опасности. Противодействието на дадена опасност е свързано с политиката на сигурност, разработена от специалистите, които реализират този защитен механизъм.

В СЕТ защитната стена се използва за филтриране на трафика и предпазване от нежелани външни приложения.

Г. Защитени сървъри и клиенти

За нормалното и сигурно протичане на транзакционните процеси е необходимо клиентските устройства и сървърите, участващи в тези процеси, да използват защитни механизми, които да гарантират за безопасното им функциониране. Тези механизми се реализират с използването на вградените защитни функции на операционната система и използването на антивирусен софтуер.

Вградени защитни функции на операционната система

Традиционен похват в клиентските и сървърните операционни системи, предлагани от Apple и Microsoft, е автоматичната актуализация на операционните системи (Laudon K. T., 2013). Производителите постоянно осигуряват актуализации на техните операционни системи с цел елиминиране на открити уязвимости и слабости. Достъпът до тези актуализации се осъществява, когато операционните системи функционират посредством интернет свързаност. По този начин клиентските и сървърните операционни системи са защитени от най-новите и най-често срещаните зловредни програми.

Използване на антивирусен софтуер

Антивирусен софтуер е общо понятие за всички типове софтуер, проектиран за предпазване и премахване на вируси и други вредителски програми (Parsons, 2013). Тези програми, известни под наименованието **malware**, основно са няколко вида - троянски

коне, червеи и вируси. Изборът на антивирусен софтуер е много отговорен процес и се свързва с детайлно запознаване с дейността на бизнес организацията, проучване на пазара на антивирусен софтуер и на критериите за избор на най-подходящ продукт.

След систематизираното представяне и анализиране на технологиите за информационна сигурност, можем да направим извода, че само някои от тях отговарят на всички изисквания за защита в ЕТ. По-подробно, това е представено в таблица 2.2.

Таблица 2.2.

Технологични решения, поддържащи измеренията на защитената транзакция в ЕТ

Измерение \ Технология	Интегритет	Неотричане	Автентификация	Конфиденциалност	Неприкосн. на личн. данни	Достъпност
Криптография	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Защитени канали за комуникация	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Защитени мрежи	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Защитени сървъри и клиенти	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

От съпоставянето на технологиите можем да направим извода, че е целесъобразно да се прилагат технологии, които да гарантират шестте измерения на електронните транзакции. Това не означава да се омаловажат предимствата на тези, които гарантират само част от тези измерения. Ние считаме, че правилният подход за избор на технологии за сигурност включва комбинация от представените такива в таблица 2.2, в зависимост от финансовите и кадровите възможности на бизнес организацията.

2.1.3. Организационни политики за управление за информационната сигурност

Разгледаните дотук решения представляват технологии за защита на информацията. Според много ИТ специалисти обаче, без наличието на разработена политика за управление на сигурността, и най-добрата технологична защита няма да бъде достатъчно ефективна. Ето защо те трябва да бъдат допълнени от политически решения. Приетите държавни закони и политическата среда също имат сериозна роля за защита от неправомерно използване на информация и злонамерени действия през Интернет.

План за изграждане на защитата в СЕТ

Съставянето на план за защита цели да се минимизират заплахите за сигурността в електронните транзакции. Отделните стъпки при разработването на този план са представени на фиг. 2.5.



Фиг. 2.5 Разработване на план за защита, източник: (Laudon К. Т., 2013)

Оценката на риска е първата стъпка от плана по сигурността. Като високо рискови компоненти и връзки между тях в СЕТ можем да определим клиентски компютър, сървър, мрежа между тях, клиентски данни и др.

Втората стъпка от процеса по разработване на плана за защита е свързана със създаване на политика за сигурност. Принципно, една политиката за сигурност предполага първо – дефиниране на набор от правила и процедури по идентифициране и систематизиране по приоритет на всички реални и потенциални рискове за компанията, второ – определяне на едно приемливо ниво за всеки риск и трето – набелязване на конкретни механизми за постигане и поддържане на това приемливо ниво на рисковете.

Подробна методология за създаване на политика за сигурност в СЕТ е разработена в глава 3, т.3.3.2.

На следващата стъпка е поставена процедура за изпълнение. Това са конкретните действия, които трябва да се изпълнят, за да се постигнат целите в плана за сигурността. Тук се определят начините, по които ще се приложат избраните инструменти, технологии, политики и процедури.

Според нас на тази стъпка от плана трябва да се проектира архитектурен модел на СЕТ, който да включва набор от технически решения, отговарящи на приетите политики и процедури. Подходящ модел предлагаме в т.3.3.4 на глава 3.

Четвъртата стъпка е свързана със създаването на организация за сигурността. На тази стъпка се обучават кадри, уведомява се управлението относно заплахи за сигурността и настъпили пробиви, поддържат се избраните инструменти, които осигуряват сигурността. Организацията по сигурността най-често се отнася до ръководенето на контрола за достъп, процедурите за автентификация и политиките за оторизация.

Последната стъпка в разработването на плана за защита е изпълнението на одит на сигурността. Одитът включва използването на рутинни отчети за начините, по които потребителите имат достъп до сайта. Чрез редовното проверяване на достъпа на потребителите до системите се цели идентифициране на подозрителни действия.

Според нас одитът на сигурността в СЕТ трябва да обхване чувствителните области като достъп до системата, предаване на данни за сметки и др. и да следи за спазването на приетите правила и процедури за сигурност, както и да изпълнява контролни функции.

2.1.4. Индустрални стандарти и нормативни актове за защита на информацията

Според международната организация по стандартизация ISO “стандартите са документирани договорености, съдържащи технически спецификации или други прецизни критерии, които трябва да бъдат използвани последователно, като правила, ръководства или дефиниции на характеристики, с цел да осигуряват необходимата реализация на предназначението на материали, продукти, процеси и услуги” (ISO, n.d.). Целта на тяхното дефиниране е да се представят механизми за защита и превенция на трите основни

компонента на информационната сигурност: достъпност, интегритет и конфиденциалност.

Използвани стандарти за информационна сигурност

За запазване достъпността, интегритета и конфиденциалността на информацията в европейски и световен мащаб са разработени и се прилагат няколко стандарта за информационна сигурност – ISO 17799:2005 / ISO 27001:2005, БДС ISO/IEC 17799:2006, Кодекс за добра практика за управление на сигурността на информацията/ БДС ISO/IEC 27001:2006, Системи за управление на сигурността на информацията ISMS и др. Тези стандарти определят изискванията, на които трябва да отговаря сигурността на информацията и на технологиите в информационните системи на дружеството или корпорацията. Стандартите, които може да се използват в СЕТ разглеждаме по-подробно в т.2.3 на настоящата глава.

Закопи, регламентиращи сигурността в електронната търговия

В резултат на развиващите се пазарни отношения, икономическата обстановка в държавата непрекъснато се променя. Като следствие на това, Интернет вече не е неконтролируема технология, а електронните пазари функционират при наличие на утвърдени закони и механизми. Целта на приеманите закони е да се осигурят условия за коректни, равноправни и регламентиращи отношения във виртуалното пространство.

В България въпросите, свързани с електронния документ, електронния подпис, условията и реда за предоставяне на удостоверителни услуги се уреждат от Законът за електронния подпис (Lex.bg, 2001). По смисъла на този закон, *електронно изявление* е словесно изявление, представено в цифрова форма чрез общоприет стандарт за преобразуване, разчитане и визуално представяне на информацията. *Електронен документ* е електронно изявление, записано върху магнитен, оптичен или друг носител, който дава възможност да бъде възпроизведено. *Автор на електронното изявление* е физическото лице, което в изявлението е посочено като негов извършител. За *титуляр на електронното изявление* се счита лицето, от името на което е извършено електронното изявление. Според същия закон, *посредник при електронно изявление* е лице, което по възлагане от титуляра изпраща, получава, записва или съхранява това електронно изявление. Отговорността за сигурността на предаваната информация се поема от посредника и според Закона за електронния подпис, той е задължен да разполага с техническо и технологично оборудване, което да осигури стабилност на използваните системи, да поддържа персонал, да притежава необходимите експертни знания, опит и квалификация, да осигурява условия за точно определяне на времето и източника на предаваните електронни изявления, да използва надеждни системи за съхраняване на информацията.

Важно място заема и правната уредба на електронния подпис, която в съответствие с нормите на ЕС следва да гарантира сигурността на информационния обмен, целостта и достоверността на съобщенията в мрежата.

Едно от основните приложения на електронния подпис е в електронните разплащания. Почти всички български банки предоставят възможност на своите клиенти за сигурно онлайн плащане чрез електронно подписване.

Напоследък широко се използват персонални идентификационни кодове - ПИК. Те се издават от Националния осигурителен институт - НОИ или от Национална агенция за приходите – НАП, като издаденият от НОИ код е 10 цифрен, а този от НАП – 12 цифрен (НСИ, n.d.). Чрез тях потребителите могат да ползват електронните услуги, предоставяни от съответната институция.

Към настоящия момент, в България все още не е усъвършенствана инфраструктурата на публичните ключове, а Законът и Правилникът за електронния подпис не са регламентиращи коректно.

Можем да обобщим, че постигането на висока степен на информационна сигурност в ЕТ е много сериозен и отговорен процес, който не се изчерпва единствено с избора на подходяща технология и нейното внедряване. Използваната технология сама по себе си не може да осигури високо ниво на сигурност, понеже в основата на механизмите за сигурност стои човешкият фактор. Постигането на високо ниво на информационна сигурност изисква също и разработването на организационни решения, в които се включват планове, политики, процедури и др. Правилното формулиране на план за защита и съставните му елементи допринася за постигането на целите на сигурността, които са поставени от компанията.

Икономическата обстановка и приетите закони оказват положително влияние при функционирането на електронните пазари, като гарантират санкции при неправомерни и злонамерени действия.

2.2. Протоколи за сигурност на информацията, използвани в системите за електронна търговия

Протоколите за сигурност на информацията представляват набор от правила за сигурно комуникиране между устройствата в дадена мрежа. Те намират приложение в СЕТ, както за процедури като удостоверяване, така и за подsigуряване на различни частни мрежи като VPN, VoIP мрежи и др., при връзките между страните на електронните трансакции.

2.2.1. Протоколи за удостоверяване

Процедурата по удостоверяване е от първостепенно значение при обмена на информация в дадена мрежа, тъй като правата в съответната мрежа се основават на идентичността на потребителя.

Основните **методи за удостоверяване** най-общо могат да бъдат класифицирани като методи за локален контрол и методи, при които се извършва удостоверяване посредством доверена трета страна, на която се разчита, за да се потвърди нечия идентичност. Потенциална слабост в методите за удостоверяване се свежда до това, на кого да се вярва. В това отношение предимство получават методите за удостоверяване посредством трета страна, поради ограничаващия фактор в силата на удостоверяването.

Като най-широко използван инструмент за удостоверяване се използват **паролите**, чието основно предназначение е да служат като доказателство за удостоверяване на потребител, софтуерен агент или устройство. За повишаване сигурността на паролите се предлагат методи за подсилване на тяхната надеждност, които включват криптиране на паролата или промяна на криптирането, така че криптираната стойност да се променя всеки път. Сходни методи се прилагат при схеми за еднократни пароли, където най-разпространени са протоколът **S/Key** и схемите за удостоверяване с контролни пароли.

Протоколът за пароли **One-Time Password System S/Key** представлява система за генериране на еднократни пароли, базирана на алгоритмите MD4 и MD5. Протоколът е разработен от Bell Communications Research (**Bellcore**) и дефиниран в Request for Comments (RFC) 1760 (Kizza. J., Computer Network Security and Cyber Ethics, 2011). Неговата цел е да устоява на риплей атаки, които се осъществяват, когато външен потребител подслушва мрежовата връзка, с цел да се сдобие с потребителското име и паролата за вход на легитимен потребител, и в по-късен момент да ги използва, за да получи достъп до мрежата.

Като инструмент за достъп, паролите са включени в множество протоколи, които осигуряват услуги за удостоверяване. Такъв е протоколът **Point to Point Protocol (PPP)**,

който се използва най-често при входящи връзки за установяване на достъп през серийна шина или мрежа за интегрирани услуги – Integrated Services Digital Network (ISDN) (Lammie, 2006). Протоколът PPP предполага стандартно капсуловане на Internet Protocol (IP) във връзки от тип точка към точка, като дава решение на проблеми от типа на присвояване и управление на IP адреси, асинхронно и битово-ориентирано синхронно капсуловане, мултиплексиране на мрежовия протокол, конфигурация на връзката, тестване на качеството на връзката, засичане на грешки и договаряне на опции за възможности като договаряне на мрежови адрес на слой и договаряне на компресия на данните. Изброените проблеми се решават с помощта на протокола Link Control Protocol (LCP) и набор протоколи - Network Control Protocols (NCPs). Механизмите за удостоверяване на PPP включват протоколите Password Authentication Protocol (PAP), Challenge Handshake Protocol (CHAP) и Extensible Authentication Protocol (EAP) (Kizza. J., Guide to Computer Network Security, 2013).

Протоколите за удостоверяване използваме в предложения архитектурен модел за защитена и сигурна връзка между електронния магазин и компанията, която го поддържа, както и за идентифициране на потребителите (вж. глава 3, т.3.3.4).

Протоколи, използващи механизми за удостоверяване

Протоколите, използващи механизми за удостоверяване изискват проверка на удостоверяването преди да оторизират и дадат права за достъп на потребители или устройства. Тук се включват протоколи като:

- **TACACS+** е базиран на **User Datagram Protocol (UDP)** протокол за контрол на достъпа (Sankar, 2005), използващ протокола TCP за комуникация и предоставя опция за обмен на удостоверяване с произволна дължина и съдържание, което позволява използването на всякакъв механизъм при TACACS+ клиентите, който може да бъде: PPP PAP, PPP CHAP, PPP EAP контролни карти. Удостоверяването не е задължително, а се разглежда като възможност, конфигурирана според случая и може да се използва само за определени услуги.

- **Remote Address Dial-In User Service (RADIUS)** е разработен като протокол за удостоверяване пред сървър при отдалечен достъп (Stewart, 2012). Той използва протокола UDP като способ за предаване на данните и се определя като услуга без установяване на връзка. Удостоверяването се реализира чрез множество методи, като функционалността за удостоверяване и оторизиране е обединена.

- **Kerberos** е разработен от масачузетския технологичен университет - Massachusetts Institute of Technology (MIT) и използва алгоритъма Data Encryption (DES) за криптиране и удостоверяване (Steudler, 2000). Той е проектиран за удостоверяване на потребителски заявки за мрежови ресурси и е базиран на концепцията за доверена трета страна, която осъществява достоверна проверка на потребителите и услугите. Доверената трета страна се нарича *център за разпространение на ключове (Key Distribution Center - KDC)* (Ec-Council, 2010), също наричана и сървър за удостоверяване. Концепцията за Kerberos включва няколко термина (Ubuntu, 2012), свързани с протокола, които са: *акредитация (credential)*; *инстанция (instance)*; *керберизиран (kerberized)*; *kerberos област (kerberos realm)*; *kerberos сървър*; *център за разпределение на ключове (key distribution center - KDC)*; *участник (principal)*; *акредитация за услуга (service credential)* *KDC TGT*; *SRVTAB*; *ticket-granting (TGT)*.

- **FORTEZZA**, заедно с приложенията, които функционират с него, предоставя услуги по сигурността за защита на ценни, но не поверителни данни (Каео, 2006). Протоколът предоставя възможности като:

- защита на данни, когато се използват от комерсиална, готова за използване работна станция в LAN или WAN среда;
- услуги за идентификация и удостоверяване, конфиденциалност, цялост на данните и отказоустойчивост;
- поддръжка на различни операционни системи на работните станции.

FORTEZZA Plus е подобрена версия на FORTEZZA, която осигурява възможност за криптиране на поверителна информация на ниво строго секретно.

За да се използва от потребителя, FORTEZZA трябва да работи с приложения, проектирани специално да бъдат съвместими с протокола. Тези приложения са разработени за правителството на САЩ, основните от които са: *електронни съобщения; world Wide Web (WWW); приложения за криптиране на файлове и данни; идентификация и удостоверяване.*

Протоколите, използващи механизми за удостоверяване са сравнени в таблица 2.3 по основни параметри. Тъй, като Kerberos се базира на концепцията за доверена трета страна, той не е включен в направеното сравнение в таблица 2.3.

Таблица 2.3

Сравнение на протоколите, използващи механизми за удостоверяване

Протоколи	RADIUS	TACACS +	FORTEZZA
Характеристики			
Транспортен протокол	UDP	TCP	–
Криптиране	Само паролата	Цялото съобщение	Цялото съобщение
Автентификация и оторизация	Обединена функционалност	Разделена функционалност	Разделена функционалност
Основна употреба	Мрежови достъп	Администриране на устройства	Развиване на системи за защита на съобщенията
Поддръжка	Множество компании	Единствено от CISCO	Множество компании

Източник: адаптирано по (Woland, 2014)

Протоколите, използващи механизми за удостоверяване като Radius, Tacacs и Kerberos, можем да използваме в предложения архитектурен модел за СЕТ за защита на връзките при отношенията бизнес към бизнес (B2B) (вж. глава 3, т.3.3.4).

В обобщение може да отбележим, че установяването на самоличността на потребителя, който изисква достъп до мрежата, е едно от най-важните изисквания за сигурност. Удостоверяването е последвано от оторизиране и контрол на достъпа, като протоколите, спомагащи тези процеси, могат да удостоверяват само крайния потребител или само крайното устройство. Поради тази причина се правят комбинации от двата типа протоколи за идентифициране и на потребителите, и на крайните устройства, с цел да се повиши сигурността на мрежата.

2.2.2. Протоколи за сигурност в слоевете на модела OSI

Моделът **Open System Interconnect (OSI)** е разработен от международната организация за стандартизация ISO и описва структурата на „свършена“ мрежова връзка, като се позовава на понятието нива на взаимодействие на мрежовите компоненти (Gupta,

2006). Моделът включва седем нива на взаимодействие, които се разглеждат като автономни и се разграничават както следва: *физическо ниво, канално ниво, мрежово ниво, транспортно ниво, сесийно ниво, представително ниво и приложно ниво*.

Протоколите за сигурност засягат приложното, транспортното, каналното и мрежовото ниво, поради което са обект на по-подробно разглеждане.

Протоколи за сигурност на приложното ниво

На това ниво се използват *end to end* протоколи за сигурност. За защита на електронните транзакции се използва Secure Hyper Text Transport Protocol (SHTTP), а за защита на софтуерни продукти за електронна поща и съобщения се използва протоколът Secure Multipurpose Internet Mail Extensions (S/MIME), който е проектиран с цел да добави функционалност за защита към протокола Multipurpose Internet Mail Extensions (MIME).

Протоколът **SHTTP** се използва за комуникация чрез защитени съобщения и е разработен специално за защита на съобщения чрез протокола HTTP (Bhasker, 2009). SHTTP запазва характеристиките на HTTP и осигурява възможност съобщенията за заявки и отговори да се подписват, удостоверяват, криптират, да се прави комбинация от трите или могат да бъдат оставени без защита.

Вторият протокол за защита на данните в приложния слой е известен с наименованието **Secure Multipurpose Internet Mail Extensions (S/MIME)** (McBee, 2010). Той е проектиран с цел да бъде лесен за интегриране в клиентски приложения за електронна поща и съобщения, като добавя защита върху стандартния протокол MIME, в съответствие със също толкова важен набор от криптографски стандарти – Public Key Cryptography Standards (PKCS).

Протоколът S/MIME притежава специфични характеристики, които го правят много гъвкаво решение за сигурност, използвано за множество приложения. Тези характеристики се отнасят до възможности за: *множество подписващи; множество получатели; разписка; препредаване; независимост от транспорта*.

Протоколите от приложното ниво предоставят различни форми на криптиране, стабилност и приложимост. Сравнение по техните основни критерии е направено в таблица 2.4.

Таблица 2.4

Сравнение на протоколите за сигурност от приложното ниво

Протокол \ Критерии	S/MIME	SHTTP
Криптиране	Базиран на RSA	Самостоятелно
Предназначение	Сигурност за протокола MIME	Сигурност чрез криптиране на отделни изпращани страници
Стабилност	Висока	Много висока
Приложимост	Да	Да

Протоколите от приложното ниво използваме в предложения архитектурен модел за СЕТ за защитена комуникация между клиента и електронния магазин (вж. глава 3, т.3.3.4)

Протоколи за сигурност в транспортното ниво

Това ниво също използва *end-to-end* протоколи, чиято цел е да осигурят защита и да предоставят методи за имплементация на конфиденциалност, удостоверяване и цялост над транспортния слой.

Първият протокол от този вид е **Secure Socket Layer (SSL)/Transport Layer Security (TLS)**. Той дефинира механизъм за защита на данните, разпределен между приложни протоколи като HTTP, FTP, TCP/ IP и др. Протоколът осигурява криптиране на данните, удостоверяване на сървъри, цялост на съобщенията и евентуално удостоверяване на клиента при TCP/ IP връзка, като основната му цел е да се осигури конфиденциалност и надеждност между две общуващи приложения. SSL е протокол със слоеве и се състои от протокола за записи и услуги за сигурност за четирите протокола за слоя данни (договаряне на криптографските параметри, съобщаване, промяна в записите за криптиране и протоколи, които дефинират клиент/сървър протоколи, притежаващи специфични портове) (Dong, 2012).

Secure Shell (SSH) е протокол за защитен отдалечен достъп и защитени мрежови услуги през незащитена мрежа (Каео, 2006). Той осигурява защитено отдалечено влизане, защитено предаване на файлове и защитено изпращане на пакети с данни. Протоколът SSH се състои от три основни компонента - протокол за транспортния слой, протокол за удостоверяване на потребителя и протокол на връзката. Имплементации на SSH са разработени за системи на Unix, Windows и Macintosh.

Протоколът **Secure Electronic Transactions (SET)** е резултат от съвместна разработка на Visa и MasterCard и има за цел да подsigури електронните транзакции през отворени мрежи като Интернет (Isaca.org, n.d.). Това се постига чрез осигуряване на конфиденциалността на информацията, гарантиране интегритета на данните относно плащания за стоки и услуги и едновременното удостоверяване на клиента и търговеца. За реализирането им се използват механизмите на криптиране, като за целите на идентифицирането се използват цифрови сертификати.

Въпреки големите му предимства, към настоящият момент протоколът не намира приложение. Вместо него, Visa прилага стандарта 3-D Secure, който ще бъде разгледан в т.2.3 в настоящия труд.

Последният, но не по важност, протокол за защита на данните от транспортното ниво е **Socket Security (SOCKS)**. Той е защитен мрежов прокси протокол, проектиран с цел да предостави рамка за клиент/сървър приложения за удобно и сигурно използване на услугите на мрежова защитна стена (Isaca.org, n.d.).

Протоколите от транспортното ниво имат различни функционални възможности. Тяхното съпоставяне е представено в таблица 2.5.

В предложеният архитектурен модел за SET използваме протоколите от транспортното ниво за сигурна криптирана връзка между страните на електронните транзакции (вж. глава 3, т.3.3.4)

Таблица 2.5

Сравнение на протоколите за сигурност от транспортното ниво

Протоколи	SSL	SSH	SET	SOCKS
Функционални възможности				
Криптиране по време на трансфер	Да	Да	Да	–

Потвърждаване на интегритета съобщенията	на на	Да	Да	Да	–
Автентификация		Само на клиента	Цялостна	Цялостна	Само на клиента
Използване на мрежова защитна стена		–	–	–	Да

Защита на мрежовото ниво

На това ниво пакетите с данни се предават през множество междинни системи, всяка от които изследва потока от пакети и го препредава към следващата система до достигането на крайната точка.

За защита на данните в мрежовия слой се използва **комплектът протоколи IP Security (IPsec)**. Този комплект съдържа набор от стандарти, използвани за осигуряване на конфиденциалност и удостоверяване на IP ниво. Сертифицираните стандарти включват четири основни спецификации, които не зависят от използваните алгоритми (Dhotre, 2010). Това са *RFC 2401 The IP Security Architecture*, *RFC 2402 The IP Authentication Header (AH)*, *RFC 2406 The IP Encapsulating Security Payload (ESP)*, *RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)*.

Наборът от услуги за сигурност на IPsec осигурява: контрол на достъпа; цялост без установяване на връзки; удостоверяване на източника на данни; отхвърляне на повторени пакети; конфиденциалност; криптиране; ограничена конфиденциалност на трафика. Тези услуги се предоставят на IP ниво и затова могат да бъдат използвани от всички протоколи от по-високо ниво.

Възможностите за защита, предоставени от протокола IPsec, в предложеният архитектурен модел за СЕТ, използваме за подsigуряване на външните комуникации на електронният магазин (вж. глава 3, т.3.3.4).

Технологии за сигурност в каналното ниво

Технологиите за сигурност в каналното ниво се използват главно за тунели, формирани за сигурно свързване на отдалечени сървъри и потребители с фирмената инфраструктура посредством локален достъп до Интернет. За тази цел се използват три основни протокола:

- Протоколът Layer 2 Forwarding (L2F);
- Point-to-Point Tunneling protocol (PPTP);
- Layer 2 Tunneling Protocol (L2TP).

Протоколът Layer 2 **Forwarding (L2F)** е създаден от Cisco Systems (Stewart, 2012). Той представя механизъм за взаимна автентификация при тунелиране, без да предлага криптиране. Протоколът не получава широко разпространение и затова скоро е заменен от Layer 2 Tunneling Protocol, който е разгледан по-напред в нашето изложение.

Вторият протокол **Point-to-Point Tunneling protocol (PPTP)** е разширение на разгледания вече Point to Point Protocol (PPP), който е бил създаден специално за достъп през комутируеми телефонни линии. Протоколът PPTP инкапсулира данните като използва PPP и след това предава IP пакети с данни през IP-базирана мрежа, каквато е Интернет или частна интранет мрежа (Network Defense: Security and Vulnerability Assessment, 2010).

Познати са три основни PPTP конфигурации - конфигуриране на сървър за приемане на PPTP- клиенти; конфигуриране на фирмени офиси с PPTP- връзки от тип шлюз-шлюз (gateway-to-gateway); конфигуриране на клиент за връзка към PPTP-сървъри.

Layer 2 Tunneling Protocol включва характеристиките на предходните два протокола L2F и PPTP, дефиниран е в RFC2661 и се използва за тунелиране на редица протоколи от други слоеве (Douligeris, 2007). Най-добрите черти на протокола PPTP се комбинират с протокола L2F (Layer 2 Forwarding) на Cisco, за да се създаде L2TP.

Point to Point Protocol over Ethernet (PPPoE) е дефиниран в RFC 2516 и служи за капсулиране на PPP пакети в каналния слой (Vermillion, 2003). Чрез него няколко хоста от една подмрежа могат да се свържат с концентратор за отдалечен достъп чрез просто мостово устройство за достъп. Този модел се използва основно в ADSL среди за предоставяне на контрол на достъпа за всеки отделен потребител.

Протоколите от каналното ниво предлагат различна степен на защита посредством криптиране, автентификация и др. Сравнение по техните основни възможности направено в таблица 2.6.

Таблица 2.6

Сравнение на протоколите за сигурност от каналното ниво

Протоколи	L2F	PPTP	L2TP	PPPoE
Критерии				
Криптиране	–	Криптира само съобщението	Целият пакет с данни се криптира	Криптиране на всички елементи в пакета
Автентификация	–	Базирана на потребителя	Взаимна автентификация чрез сертификати	Базирана на потребителя
Преобразуване на мрежови адреси	Не се срещат проблеми	Не се срещат проблеми	Възможни са проблеми, когато се използва IPsec	Възможни проблеми при конфигуриране на рутери

Сравнените по-горе протоколи от каналното ниво намират приложение при виртуалните частни мрежи, които в предложеният модел за СЕТ можем да използваме за защитена комуникация при отношенията бизнес към бизнес (B2B).

Можем да обобщим, че за защита на данните, които преминават през корпоративната мрежа, се използват множество технологии на различните нива. Всяка технология има своите предимства и може да бъде използвана, в зависимост от конкретните условия. Протоколите за сигурност от приложното ниво се отличават със своята гъвкавост към конкретното приложение, което допринася за тяхната приложимост, но в някои ситуации използването им може да се окаже непрактично. Протоколите от транспортното ниво имат широка приложимост, най-вече протоколът TLS, който се използва в повечето уеб сървъри и клиенти и се е наложил като стандарт за защита на електронните транзакции. На мрежовото ниво протоколът IPsec дефинира услуги за сигурност на IP ниво, базирани на комбинация от IP адрес, транспортен протокол и приложение. Протоколите от каналното ниво, които имат редица предимства и предоставят механизми за сигурна комуникация с корпоративната мрежа през Интернет, са в основата на виртуалните частни мрежи.

2.2.3. Протоколи за защита на информацията при различни видове частни мрежи

Виртуални частични мрежи (Virtual Private Networks – VPN)

VPN, както вече беше споменато (вж. т.2.1.2), представляват сигурни частни мрежови връзки от точка до точка, използващи инфраструктура на публична мрежа чрез тунелиране (Whitman M. H., 2009).

В практиката се използват четири протокола за VPN тунелиране: IP Security (IPsec), Point to Point Tunneling Protocol (PPTP), Layer2 Tunneling Protocol (L2TP) и Layer 2 Forwarding (L2F) (Singh, 2012). Въпреки че съществува схващането, че тези протоколи са конкуриращи се технологии, те предлагат различни възможности, които са подходящи за различна употреба.

Виртуалните частни мрежи с широки мащаби изискват предимно използването на протокола IPsec или комбинация от L2TP и IPsec, за да предоставят услуги за сигурност. Някои организации предпочитат да използват само PPTP или L2TP, но тъй като IPsec предоставя цялостни услуги за сигурност, този протокол задължително трябва да присъства в повечето сигурни VPN решения.

Виртуалните частни мрежи с описаните вече протоколи в предложения архитектурен модел за СЕТ намират приложение за сигурна криптирана връзка в отношенията бизнес към бизнес (B2C) (вж. глава 3, т.3.3.4).

Сигурност на безжичния достъп до системите за електронна търговия

Безжичните мрежи предоставят мобилност на мрежовите потребители и осигуряват удобството на лесната инсталация, избягвайки скъпо струващото полагане на физически кабели. С масовото разпространение на преносимите компютри и устройства (лаптопи, смартфони, таблети), безжичните мрежи се превърнаха в основен способ за достъп за повечето клиенти.

По настояще съществуват няколко стандарта за Wireless Local Area Network приложения (Qin, 2009). Те са:

- **Hiper LAN - High Performance Radio LAN** - Стандарт на European Telecommunications Standards institute (ETSI), ратифициран през 1996 г.
- **Home RF SWAP - Shared Wireless Access Protocol (SWAP)** - протокол за безжична комуникация между персонални компютри и устройства от битовата електротехника в дома.
- **Bluetooth** – Personal area network (PAN) – технология, разработена от Bluetooth Special Interest Group за предоставяне на безжична връзка на малко разстояние посредством превключване на честоти и за спектърно разпростиране в честотната лента на 2.4GHz.
- **802.11** - безжичен стандарт, определен от IEEE. Съществуват няколко спецификации: **802.11 b** - наричана също и Wi-Fi (Wireless Fidelity) и поддържа до 11 Mbps в честотната лента от 2.4 GHz; **802.11 a** - предоставя възможност за комуникации със скорости до 54 Mbps на 5,8 GHz; **802.11 g** - разширява още повече възможностите на безжичните комуникации при 54 Mbps на 2,4 GHz и има обратна съвместимост с 802.11b; **802.11 n** - поддържаща скорости до 600 Mbps; **802.11 i** - специфицира сигурни механизми за безжичен достъп **Wi-Fi Protected Access (WPA)** и WPA2, които са разработени да заместят стандарта WEP поради слабостите му (Halapacz, 2011); **802.11 e** - допълва протоколите за безжичен достъп и осигурява предаването на мултимедия; **802.11 f** - определя комуникация между възли, като поддържа Inter Access Point Protocol (IAPP) за 802.11; **802.11 h** - прилага се като технология за спектрално управление на 802.11 a.

Основен проблем по отношение на сигурността при безжичните мрежи е осъществяването на сигурен достъп до точката на достъп, която свързва безжичното устройство с локалната мрежа и възможност за изолирането ѝ от вътрешната частна мрежа преди удостоверяване на потребителя в мрежовия домейн.

Въпреки множеството достойнства на оригиналната 802.11 спецификация, механизмите за сигурност показват редица слабости и по тази причина е дефиниран нов стандарт IEEE 802.11i, който подобрява сигурността на безжичния LAN (Rittinghouse, 2004). Усъвършенстването на защитата включва протоколите **Temporal Key Integrity Protocol, EAP Transport Layer Security, EAP-Tunneled TLS, EAP-Cisco Wireless (LEAP) и Protected EAP.**

Протоколите за защитен безжичен достъп имат широко приложение, особено в онлайн пазаруването. Основните им функционални възможности са обобщени в таблица 2.7.

В предложения архитектурен модел за СЕТ, протоколите за защитен безжичен достъп намират приложение при комуникациите между клиентите на електронния магазин и доставчика на Интернет услуги, както и при електронни разплащания от мобилни устройства (вж. глава 3, т.3.3.4).

Таблица 2.7

Сравнение на протоколите за сигурност при безжичен достъп

Протоколи Възможности	WEP	EAP TLS	EAP TTLS	LEAP	PEAP	TKIP
Динамична промяна на ключове	–	Да	Да	Да	Да	Да
Взаимна автентификация	Да	Да	Да	Да	Да	Да
Изискване за сървърни сертификати	Да	Да	Да	Да	Да	Да
Изискване за клиентски сертификати	–	Да	–	–	Да	–
Тунелиране	–	–	Да	–	Да	–
Собствен стандарт	–	–	–	–	–	–

Източник: (CISCO, n.d.)

Защита на данните при Voice over IP мрежи (VoIP)

Voice over IP (VoIP), наричано още **IP телефония**, представлява осъществяване на телефонни разговори през IP мрежа. VoIP добиват широко приложение благодарение на цялостните технически стандарти и решения, които редуцират разходите за поддръжка на мрежа и усъвършенстваните комуникации в бизнеса. Основните компоненти на VoIP мрежа включват (Components of a VoIP network, n.d.):

- агент на обажданията – всяко устройство, което може да извършва или да приема разговори;
- портал – устройства, които изпълняват ролята на мост между VoIP и Public Switched Telephone Network (PSTN) мрежа;
- прокси сървър, който извършва маршрутизиране на обажданията, регистриране и осигуряване на достъп до мрежата.

Проектирането на VoIP мрежи се базира на три основни стандарта - H.323, Media Gateway Control Protocol (MGCP) и Session Initiation Protocol (SIP) (Sattar, 2008), (Ohrtman, 2004), (Davidson, 2007).

От изброените само H.323 и SIP имат отношение към защитата на данните в VoIP мрежите.

Сигурност при протокола H.323

За постигане на високо ниво на сигурност и защита на H.232 и H.245 мултимедийни терминали, Международното обединение за телекомуникации (International Telecommunication Union - ITU) разработва препоръката H.235, която включва възможност за договаряне на услуги и функционалност по общ начин и за избор по отношение на използваните криптографски техники и възможности.

Сигурност на протокола SIP

Протоколът SIP не дефинира нови механизми за сигурност, а използва повторно съществуващи модели за сигурност, взети от HTTP и Simple Mail Transfer Protocol (SMTP). Основните услуги за мрежова сигурност, изисквани от SIP, включват запазване на конфиденциалността и целостта на съобщенията, предотвратяване на атаки с повторения или подмяна на съобщения, предоставяне на удостоверяване и конфиденциалност на участниците в сесията и предотвратяване на атаки за отказване на услуги.

Протоколите за сигурност при IP телефония се използват в множество приложения за сигурни VoIP комуникации. Основните им възможности са представени в таблица 2.8.

Протоколите за VoIP сигурност могат да намерят приложение в предложения архитектурен модел за СЕТ в отношенията клиент към бизнес при защитени комуникации с лоялни или преференциални клиенти, а също и при B2B отношенията (вж. глава 3, т.3.3.4).

Таблица 2.8

Сравнение на протоколите за сигурност при VoIP Мрежи

Възможности	Протоколи	H.323	SIP
Автентификация		Чрез препоръката H.235	Чрез HTTP, SSL, S/MIME
Поддръжка на защитни стени		Да	–
Услуги		През уеб браузъра	Не се предоставят през уеб браузъра
Адресиране		Гъвкаво	Единствено по URI
Фактуриране		Поддържа се	Не се поддържа
Комплексност		Висока	Ниска

В обобщение можем да направим извода, че виртуалните частни мрежи, със своите механизми и технологии, предоставят най-надеждните решения за сигурност при комуникациите на организацията с външни потребители и устройства. Безжичните мрежи и мрежите за IP телефония непрекъснато се развиват по отношение на сигурността и по тази причина в определени случаи потребителите на тези мрежи имплементират собствени мерки за сигурност с цел да посрещнат пазарните нужди.

Сравнението на протоколите за защита на информацията по основни критерии е направено в таблица 2.9 (вж. приложение 2).

2.3. Сравнителен анализ на стандартите за информационна сигурност, прилагани в електронната търговия

Информационните технологии постоянно увеличават своя обхват и значение. Те променят всички сфери на бизнеса - от управлението на единични процеси до управление на цялата организация. На този фон е логична сериозната загриженост за защитата на информацията като основен ресурс на всяка организация. В това отношение е нужно стандартизиране на организациите т.е. прилагане на водещите стандарти за информационна сигурност, които са съобразени с най-новите постижения в ИКТ и мениджмънта.

В настоящата част на разработката ще разгледаме световно признатите стандарти: *ISO 27001*, *ISO 19011*, *BS7799/ISO 17799*, *ISO 27002*, *Стандарт ISO/IEC 15408*, *Американска "Оранжева книга"*, *Европейска "Бяла книга"*, *Payment Card Industry Data Security Standard*, *EMV*, *Стандарт 3-D Secure*.

Като един от основните стандарти за информационна сигурност, **ISO 27001** представлява съвкупност от изисквания за разработване на система за управление на информационната сигурност (СУИС) (СИО, Одит на Информационната сигурност - обхват, стандарти, добри практик, 2007). Пълното му наименование е Информационни технологии – техники за сигурност – система за управление на информационната сигурност – изисквания (Information technology – Security techniques – Information security management system – Requirements). Целта му е да служи за разработване, имплементиране, използване, наблюдение, поддържане и подобряване на модел на система за управление на информационната сигурност. Стандартът ISO 27001 възприема модела PDCA (Plan-Do-Check-Act). Този модел се състои от 4 стъпки: планиране, изпълнение, оценяване на резултата, предприемане на коригиращи действия. Известен е също като цикъл на **Шухарт** на името на Уолтър Шухарт, който прилага модела с цел осигуряване на постоянно усъвършенстване на системите за управление на качеството.

Последната версия на стандарта – **ISO 27001:2013** е публикувана през месец септември 2014 г. (ISO, ISO/IEC 27001:2013, n.d.) Новият стандарт поставя акцент върху измерването и оценката на това колко добре организация е изпълнявала системи за управление на информационната сигурност и има нов раздел за аутсорсинг, което е отражение на факта, че много организации разчитат на трети лица за предоставяне на някои аспекти от ИТ. Съществено за него е, че той не набляга на цикъла Plan-Do-Check-Act, както предишната му версия - ISO 27001: 2005.

Важно е да отбележим, че осигуряването на информационна сигурност е процес, който продължава във времето и трябва непрекъснато да се оценява и усъвършенства. Поради това една от ключовите характеристики на системите за управление на информационната сигурност е непрестанният мониторинг, оценяването и подобряването на системата през всички фази от разработването ѝ. Тези етапи включват дефиниране на цел и обхват, избор на методология за оценка на риска и критерии за риск и изработване на документ за пригодимост на контролните дейности (СИО, Внедряването на системи за управление на информационна сигурност – етапи и предизвикателства, 2009).

Основното преимущество на сертифициране на една организация по ISO 27001 е, че гарантира на клиентите, персонала, управлението и собствениците на компанията, че работната информация е стабилно защитена и системата за управление на тази защита е подходяща и функционираща (CSB, n.d.). Сертифицирането означава също, че организацията е наясно и включва всички правни и регулиращи изисквания, които имат отношение към нея и сектора, в който действа. Не на последно място, сертифицирането по ISO 27001 доказва, че ангажираността към информационната сигурност е налице за всички нива в организацията.

Осигуряването и поддържането на оптимално ниво на защита на информацията е процес, който изисква непрекъснат контрол, оценка и действия за усъвършенстване. **Одитирането** на информационната сигурност в организацията, което гарантира ефективността на имплементираната СУИС е един от начините за постигане на това. Периодични одити откриват различни несъответствия със стандарта или неефективно действащи контролни дейности. В такива случаи при одита се дават препоръки за подобряване на контролните дейности или за отстраняване на несъответствията със стандарта.

Стандарт, който е приложим при одитиране на системи за управление на информационната сигурност, е разработен от Международната организация по стандартизация (ISO, International Organization for Standardization, n.d.). Стандартът е известен като **ISO 19011** „Указания за одитиране на системи за управление на качеството и/или околната среда“ (Guidelines for quality and/or environmental management system auditing (Tricker, 2002)), като последната версия на стандарта е **19011:2011** – (Guidelines for auditing management systems – указания за одитиране на управленски системи (ISO, ISO 19011:2011, n.d.)). В процеса на одит съгласно стандарта ISO 27001 се извършва проверка на две ключови групи изисквания, които са:

- изисквания към процесите на системата за управление на информационната сигурност;
- указател с контролни дейности, които стандартът осигурява.

Стандарт BS 7799/ISO 17799

BS 7799/ISO 17799 е международно приет стандарт, прилаган в повече от 80 000 компании, сред които са Fujitsu Ltd, Marconi Secure System, Samsung Electronics Co Ltd, Sony Bank Inc и др. Основната му цел е постигане на сигурност и защита на информацията в една организация. Той служи като база за определяне на съвкупност от механизми за контрол, необходими за коректното използване на информационни системи в сфери като промишленост и търговия. Стандартът може да бъде използван от всяка организация, която обработва чувствителна информация, или която се стреми към високо ниво на сигурност.

Насоките, предложени от на стандарта, обхващат различни страни на сигурността като: планиране на кризисни ситуации; физическа сигурност; аспекти на сигурността по отношение на персонала; контрол на достъпа до информационните системи; сигурност при разработка и поддръжка на информационни системи.

Успешното внедряване на стандарта в дадена организация преминава през три фази - планиране, проектиране и прилагане (Ипотпал противодействие и ипотпал защита, n.d.).

Стандартът е съставен от две основни части - код на практиката - ISO 17799 и спецификация за система за управление на информационната сигурност (СУИС) и защита - BS 7799-2 (Станев, n.d.).

Първата част съдържа насоки за постигане на информационна сигурност, а втората част представя мерки за ефективно управление на информационната сигурност.

Стандартът е структуриран в 10 основни раздела, насочени към различни области. Тези раздели са:

- непрекъснато бизнес планиране;
- система за контрол на достъпа;
- разработване и поддържане на системата;
- физическа и екологична защита;
- съответствие;
- защита на персонала;

- защита на организацията;
- управление на компютрите и операциите;
- класификация и контрол на активите;
- политика на сигурност и защита.

Към настоящия момент стандартът BS 7799/ISO 17799 вече не се използва самостоятелно. Неговите препоръки са включени в серията стандарти ISO 27000 и основно в стандарта ISO 27002.

Стандарт ISO 27002

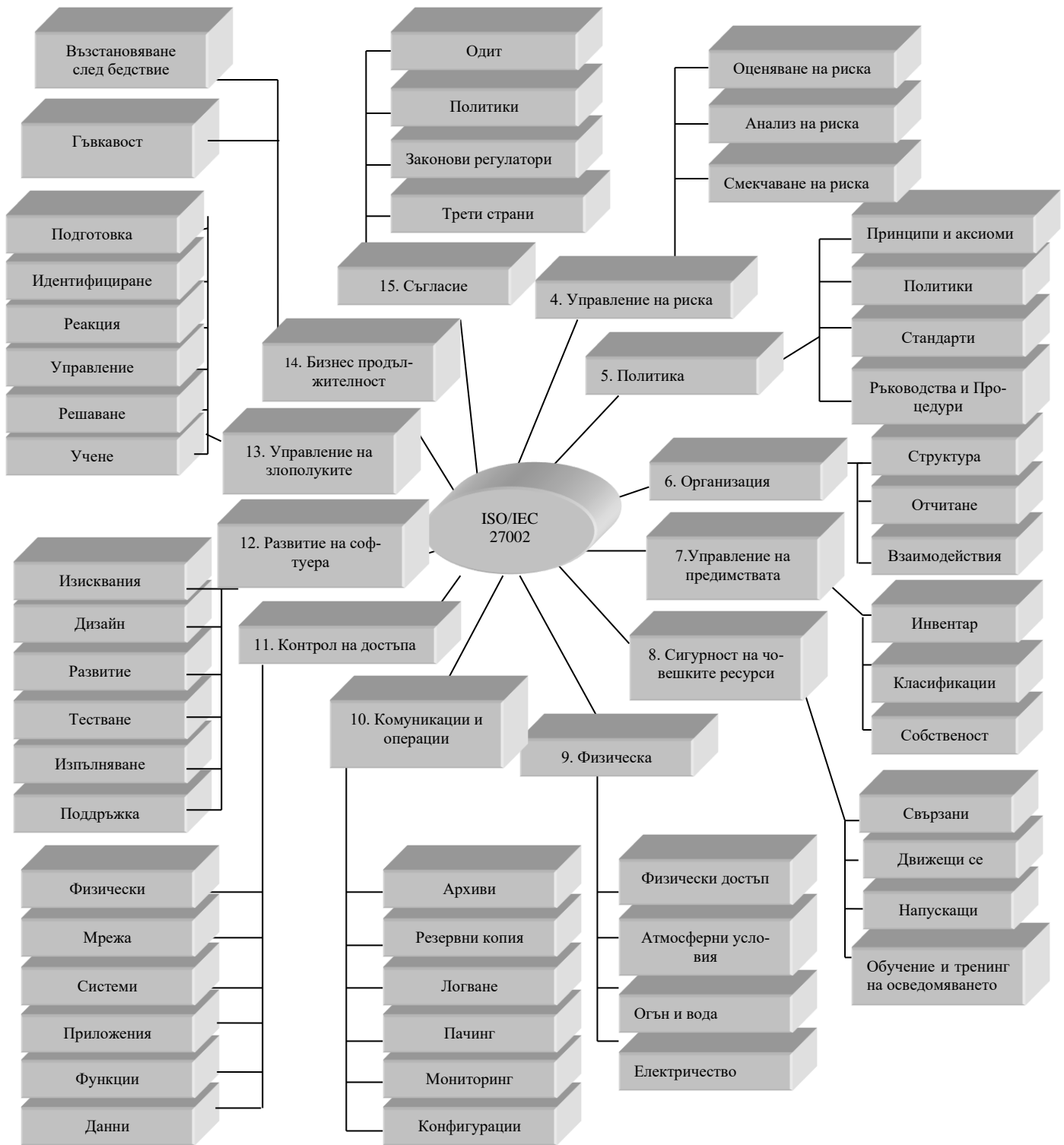
Това е международен стандарт, който предоставя насоки и подходи за изграждане, поддържане, усъвършенстване и администриране на информационната сигурност в организациите. Актуалната версия на стандарта е под наименованието **ISO 27002:2013** (ISO, ISO/IEC 27002:2013, n.d.).

Съществува възможност стандартът да се използва като практическо указание за разработване на стандарти за информационна сигурност, както и на ефективни механизми за управление на сигурността и подпомогне разработването на защита за критичната информация. Стандартът ISO/IEC 27002 изисква точно следване на закони, подзакони и договорни задължения по отношение на сигурността на информацията, оптимално потребление на ресурсите, а също и периодични проверки на системата с цел непрекъснато усъвършенстване. Схематично съдържанието на стандарта ISO/IEC 27002 е представено на фиг. 2.6.

Сертифицирането на една СУИС, съгласно ISO/IEC 27002 доказва, че организацията гарантира във възможно най-висока степен: сигурността на личната и клиентската информация; отказоустойчивостта на бизнес процесите, в случаи на извънредни ситуации и кризи (Eurox-bg, n.d.).

Разгледаният стандарт е приложим за търговски, нетърговски, правителствени и неправителствени организации, както масово в практиката се използва подходът на изграждане на СУИС, на база изискванията на **ISO/IEC 27001** и на практиките, заложи в **ISO/IEC 27002**. Формираните на база този подход СУИС имат широк обхват и покриват множество аспекти на информационната сигурност:

- оценка и управление на риска;
- управление на персонала;
- физическа сигурност;
- контрол на достъпа;
- сигурност при избора, придобиването и използването на софтуер и хардуер.



Фиг. 2.6. Съдържание на Стандарта ISO 27002, източник: (ISO, ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management, n.d.)

Американска "Оранжева книга"

Оранжевата книга е публикувана през август 1983 г. с названието критерии за оценка на защитени компютърни системи (Trusted Computer System Evaluation Criteria - TCSEC). Тя е дело на Националния център за компютърна сигурност (NCSC), който е част от Националната агенция за сигурност на САЩ (NSA). Този набор от стандарти дефинира: основните класове, понятията и критериите за оценяване степента на защитеност на компютърните системи. Оранжевата книга се явява първият набор от стандарти, използвани за класифициране и оценяване на информационната сигурност на компютърни системи (Kizza. J., Computer Network Security and Cyber Ethics, 2011). Тя дефинира основните *нива на сигурност*, които се обозначават с буквите А, В, С и D и индекси към тях. Те са класифицирани в четири раздела, всеки от които включва един или няколко класа. В последствие стандартът заместен от **ISO/IEC 15408 – Common criteria**.

Стандарт ISO/IEC 15408

Стандартът ISO/IEC 15408, популярен под названието „Общи критерии“ (Common Criteria, CC), е изграден от три части:

- въведение и основен модел - ISO/IEC 15408-1;
- функционални изисквания за сигурност ISO/IEC 15408-2;
- уверителни компоненти за сигурност - ISO/IEC 15408-3.

Последните версии на стандарта са: ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2005 и ISO/IEC 15408-3:2008. Важно предимство на стандарта е, че той представлява база за оценка на информационната сигурност и за създаване на предпоставки за съпоставяне на резултатите от изцяло независими оценки (СЮ, Ролята на международните стандарти, 2002). За постигането на тази цел се дефинира съвкупност от изисквания към гарантиращите сигурност функции и така се формира обща критерийна база за оценка.

Стандартът ISO/IEC 15408 дефинира основни елементи за осигуряването на информационна сигурност, като защитен профил, цели на сигурността, цел на оценяването, съвкупност от нива на удостоверяване при оценката на нивата на сигурност.

Стандартът дефинира две групи изисквания – *функционални*, насочени към функциите за сигурност и механизмите, които ги изпълняват; и *изисквания за доверие*, които имат отношение към методологията и процедурите по създаване и експлоатация на сигурността. Също така дефинира три вида *структури на изискванията*: *пакет*, *профил на защитата* и *задание за сигурност*, които са насочени към различни функции на организацията (Глазков, n.d.).

Друга особеност на стандарта ISO/IEC 15408 е, че дефинира *четири етапа от жизнения цикъл* на дадения обект, в съответствие с които сигурността се определя динамично:

1. определяне на предназначението, условията на използване и изискванията за сигурност;
2. проектиране и разработване;
3. тестване, оценка и сертификация;
4. внедряване и експлоатация.

Европейска "Бяла книга"

Представя набор от стандарти за сигурност, разработени на базата на критериите, дефинирани от група европейски страни, познат под наименованието "Критерии за оценка на сигурността на информационни технологии" (Information Technology Security Evaluation Criteria, ITSEC) (Information Security and Privacy in Network Environments, 1994). Според този стандарт, информационните системи най-напред трябва да осигуряват определени функции за защита, включващи:

- идентификация и автентификация на потребителите;
- контрол на достъпа;
- наблюдаване и протоколиране на събитията;
- изчистване на обектите от данните, преди да се използват повторно, за да се предотврати получаването на достъп на случайни потребители до информация, за която нямат правомощия;
- възстановяване при грешки;
- осигуряване на всички услуги за поддържане на сигурността;
- защита на данните при предаване, където се включва първоначална автентификация, контрол на достъпа, конфиденциалност на данните, цялостност на данните, автентичност на данните и безотказност.

ITSEC определя десет нива на функционалност (F1-F10) за изискванията в специфични приложения (F1 е най-ниската оценка на защита), а също дефинира и 6 нива на гарантирана коректност на функциониране на защитата (Fisch, 2000).

Payment Card Industry Data Security Standard (PCI DSS) е световно признат стандарт за сигурност, специализиран за защита на информацията при разплащане с банкови карти (Baet, n.d.). Той представя изисквания относно: контрола на сигурността, компонентите на мрежата, дизайна на софтуера, изискванията за сигурност и други механизми за защита на данните, отнасящи се за клиентската сметка. Стандартът може да се приложи за всяка компания, която съхранява, предава и обработва данни за клиентски карти.

PCI DSS се основава на 6 принципа, които обхващат 12 специфични изисквания. Те са:

- *изграждане и поддържане на сигурна мрежа*
 - инсталиране, конфигуриране и поддържане на защитна стена за защита на данните на картодържателите;
 - да не се използват основните данни на картодържателя като системни пароли и други кодове за сигурност.
- *съхраняване данните на картодържателя;*
 - съхраняване на всички данни на картодържателите;
 - криптиране на трансмисията на данните на картодържателя през отворени, публични мрежи.
- *разработване на план за управление на уязвимите места*
 - използване и актуализиране на антивирусен софтуер;
 - разработване на допълнителни системи за сигурност.
- *създаване на строг контрол за достъп*
 - стесняване на достъпа до данните на картодържателите само за обслужващия персонал, на който е необходим такъв достъп;
 - предоставяне на всеки потребител достъп с уникален идентификационен номер;
 - ограничаване на физическия достъп до данните за притежателите на банкови карти.
- *проследяване и редовно тестване сигурността на мрежата*
 - проследяване на всички свързвания с мрежата и данните на картодържателите;
 - периодично тестване на сигурността на системата и отделните процедури.
- *поддържане на информацията за сигурността на системата*

Сравнение само на съпоставимите стандарти по ключови критерии е направено в таблица 2.10.

Таблица 2.10,

Сравнение на стандартите за информационна сигурност

Категория на сигурността	ISO 15408	ISO 27002	ISO 27001	BS7799	PCI DSS
Достъпност	Да	Да	Да	Да	Да
Интегритет на данните	Да	Да	Да	Да	Да
Интегритет на системата	Да	Да	Да	Да	Да
Конфиденциалност	Да	Да	Да	Да	Да
Отчетност	Да	Да	Да	Да	Да
Застраховане	Да	Да	Да	Да	Да
Идентификация и именуване	Да	Да	Да	Да	Да
Управление на криптографски ключове	Не	Да, непреяко	Да	Да	Да
Администриране на сигурността	Да	Да	Да	Да	Да
Контрол на сигурността	Да	Да	Да	Да	Да
Защитени комуникации	Да, непреяко	Да	Да	Да	Да
Автентификация	Да	Да	Да	Да	Да
Оторизация	Да	Да	Да	Да	Да
Осигуряване на контрол на достъпа	Да	Да	Да	Да	Да
Неотричане	Да	Да, непреяко	Да	Да	Да
Конфиденциалност на транзакцията	Да, непреяко	Да	Да	Да	Да
Одит	Да	Да	Да	Да	Да
Откриване на нарушения и възпирането им	Не	Да, непреяко	Да	Да	Да
Доказателство за цялостност	Не	Не	Да	Да	Да
Възстановяване към състояние на сигурност	Не	Не	Не	Не	Не

Категория на сигурността	ISO 15408	ISO 27002	ISO 27001	BS7799	PCI DSS
Физическа сигурност	Да	Да	Да	Да	Да
Сигурност на персонала	Да	Да	Да	Да	Да

Източник: (Comparison of Information Security Standard, н.д.)

Стандартите *EMV* и *3-D Secure*, както *PCI DSS* имат пряко отношение към сигурността при транзакции с използване на банкови карти.

EMV е международен стандарт за операции с банкови карти с чип, разработен съвместно от Europay, MasterCard и Visa с цел да подобри сигурността на финансовите транзакции (Vtb-bank, n.d.). Това, което намалява риска от фалшифициране на картата, е включването на активни механизми за самостоятелно удостоверяване, базирани на асиметрична криптография в стандарта. Системите за идентификация на чип-картите - Static data authentication (SDA), Dynamic data authentication (DDA) и Combined Data authentication (CDA) при всяко идентифициране генерират уникален подпис – защита, която може да бъде преодоляна изключително трудно. Спецификациите на EMV са базирани на серията стандарти ISO 7816 и предлагат две нива на изисквания (Atkins, 2004):

- ниво 1, което покрива интерфейса на терминалния чип;
- ниво 2, което покрива приложението за плащане.

Неефективността на EMV по отношение на заплахите, свързани с несъществуващи карти, се преодолява с въвеждането на стандарта 3-D secure, който решава тези проблеми. Тази теза е подкрепена от Джонатан Ханкок, директор мениджмънт решения срещу измами към Total System Services (Rizzo, n.d.).

3-D Secure е стандарт, използван в разплащанията с кредитни и дебитни карти за онлайн защита на самоличността (UBB, n.d.). Сам по себе си той представлява схема за проверка на автентичност, при която идентичността на всяка от страните, участващи в транзакционния процес се удостоверява пред другата страна. Автентификацията на картодържателя се реализира чрез обмен на секретна информация или парола, с помощта на която на картодържателя се предоставя възможност за уникална идентификация пред издателя на картата, след което издателят удостоверява тази идентичност пред търговеца.

Наименованието “3-D Secure” произхожда от обезопасената комуникация между три домейна: издател, международни картови организации и акцептор, т.е. това е модел на взаимодействие между три независими страни.

Можем да обобщим, че ролята и значението на стандартите за информационна и компютърна сигурност е ключова при осъществяването на бизнес процесите. Защитата на информацията се осигурява от всички хора в организацията, а не само от различни технологии и мерки. Всички управленски дейности в една СУИС трябва да се предприемат на основа на оценката на риска. Системата трябва да е ресурсно осигурена и ръководството на организацията трябва да е ангажирано с въпросите за сигурността на информацията. Според Е. Лииканен, Европейски комисар, отговарящ за Европейския Икономически и социален комитет, "Развитието на електронния бизнес в Европа и в световен мащаб ще бъде насърчено и ускорено, ако съществува сигурна инфраструктура. Европейските Организации за Стандарти (ESO) ще изпълнят своята водеща роля за създаването на тази сигурна инфраструктура".

2.4. Технологии за реализиране на защитени електронни разплащания

Практиката показва, че към настоящия момент са разработени множество програми за защита на потребителите на най-големите електронни магазини в световен мащаб, което внася сериозно ниво на сигурност и способства за разпространението на мобилните системи за разплащане. Някои от по-важните са:

Програма за защита на клиентите **Ebay Buyer Protection**

Представява система за защита за клиентите на сайта за продажби Ebay, в случай на измама или незадоволителни сделки. Ebay Buyer Protection е процес на решаване на спорове, който предпазва пазарували от сайта на Ebay от некоректни сделки (Miller, 2011). Той обхваща стоки, закупени на Ebay, които или не са били получени или за тях липса описание в каталога с продукти. Купувачите, които са жертви на този вид измами, имат възможност да им се върне цялата стойност, която са заплатили за стоката.

Трябва да отбележим, че системата Ebay Buyer Protection е изпълнима, само ако са налице няколко предпоставки (Ebay, n.d.):

- плащането за стоката да е извършено с PayPal;
- в случай, че стоката не пристигне или има разминаване в описанието ѝ с това на сайта на Ebay, клиентът трябва незабавно да се свърже с представители на електронния магазин;
- уведомяването на продавача става от представителите на Ebay, които след контакта с него ще се свържат и с клиента;
- в случай, че плащането не е извършено с PayPal, представителите на Ebay могат да окажат съдействие за разрешаването на проблема.

Защита на клиентите също осигурява и системата **PayPal Buyer Protection**, която е свързана с описаната Ebay Buyer Protection и също гарантира възстановяване на цялата сума, в случай на измама, липса или получаване на стока, която не отговаря на описанието в електронния магазин (Paypal, n.d.). Както в Ebay Buyer Protection, тук също е необходимо наличието на определени условия за да функционира системата. Когато покупката е извършена от Ebay, за клиента се предоставя защита в случай на недоставена стока, или стока за която липса описание. Съществува възможност за възстановяване на заплатената сума и когато покупката не е извършена през Ebay, но това е валидно единствено в случаите, когато стоката не е доставена.

Китайски сайтове за ЕТ, които получиха широка популярност през последните години, също предлагат множество механизми за защита на информацията и на потребителите. Такива са електронните магазини от Alibaba Group, в които е имплементирана политика за сигурност, отнасяща се за всички продукти и услуги, предлагани от електронния магазин (Alibaba, n.d.). Тази политика определя начина, по който може да се събира, използва и разкрива информация към потребителите на сайта, а също дефинира правила за сигурност при мобилен достъп. Налице е и система за защита на потребителите, която гарантира пълно възстановяване на преведената сума при неизпълнение на поръчката. За защита на електронните разплащания се използва системата **Escrow**, която е част от **Alipay** - най-голямата платежна система в Китай, свързана с електронните магазини от Alibaba Group. Системата задържа плащания на купувачите, докато поръчките се обработват и стоките се доставят. След като купувачът и доставчикът са установили, че сделката е завършена, се пускат парите.

Сигурност чрез Google Wallet

Защитните механизми, наречени **Google Wallet Fraud Protection** покриват 100% от регистрираните неоторизирани портфейл сделки на Google в САЩ, което се извършва чрез система за денонощно наблюдение, даващо гаранция за спокойно пазаруване (Google, n.d.).

Google Wallet осигурява защита, еквивалентна на тази с използване на физическа карта при най-посещавани електронни магазини или още по-високо ниво на сигурност, като се използва токен устройство, с което откраднати карти стават безполезни (Androidcentral, n.d.). Инсталирането на приложението Google Wallet е съпроводено с поставянето на PIN код, който отключва портфейла за покупки, теглене на пари или разплащания, което гарантира, че само собственика на устройството ще може да оперира с портфейла. Също така приложението предоставя възможност за проследяване на поръчките, като потребителят може да откаже дадена поръчка, или да я променя. Предвидена е и възможност при кражба или загубване на потребителското устройство, потребителят да деактивира приложението от своя акаунт в Google.

Системата за разплащане Apple Pay

Чрез Apple Pay се защитават личните данни, данни за сделки и информация за кредитни и дебитни карти с водещи технологии за сигурност (Apple, n.d.). Системата също е предназначена за защита на лични данни, без да събира информация за сделките, които могат да бъдат свързани клиента. Тези операции се извършват между купувача, търговеца и банката на купувача.

Основните механизми за сигурност, които използва системата Apple Pay включват пароли, пръстови отпечатъци и криптиране.

Разплащанията в магазини, които приемат безконтактни плащания с Apple Pay, се реализират чрез технологията **Near Field Communication (NFC)** между устройството и терминал за плащане.

Amazon Payments

Използването на тази разплащателна система се осъществява чрез акаунт, който се подлага на редица процедури за проверка, за да се поддържа най-високо ниво на сигурност, доверие, и защита (Amazon, n.d.).

За гарантиране на сигурността, Amazon Payments също използва Secure Socket Layer (SSL) с 128-битово криптиране, който е индустриален стандарт в сигурната защита на сървъра. В допълнение на това, клиентската сметка се защитава с уникално създадена от потребителя парола, която трябва да отговаря на определени изисквания.

Приложението CellumPay

CellumPay е безплатно приложение, функциониращо на мобилни устройства с операционни системи IOS, Android и Windows phone, което предоставя възможност за разплащане и пазаруване чрез смартфон. Приложението е проектирано с цел елиминират всички рискове за личните данни на потребителя. Сигурността на банковите карти се гарантира чрез специфични механизми и процедури на криптиране, стриктното изпълнение на които са последвани от достъп до клиентските сметки (Investor, n.d.).

Система за електронни разплащания ePay

Системата ePay е създадена през 2000 г. и е част от „Датамакс Системс Холдинг“ АД, което е със сериозен опит в производството на банков софтуер и изграждане на платежни системи (ePay.bg, n.d.).

За защита на потребителските данни се използва HTTPS криптирана връзка, също така и механизми за сигурност като застраховка срещу злоупотреби, безплатни цифрови сертификати за контрол на достъпа в ePay, използване на електронни подписи и плащане чрез SMS код.

Приложението Mobb

Представява платформа за сигурни мобилни плащания, оперирана от „БОРИКА – БАНКСЕРВИЗ“ АД (Mobb, n.d.). Използваните технологии за информационна сигурност в mobb се основават на Public Key Infrastructure (PKI), която осигурява криптирана връзка и цялост на данните. Сигурността на приложението се допълва от факта, че данните за потребителските карти не се съхраняват в преносимото устройство. Приложението mobb поддържа всички мобилни платформи от 2004 г. до настоящият момент.

В обобщение можем да заключим, че системите за защитени електронни разплащания предоставят едно сериозно ниво на сигурност на информацията, което се постига чрез криптиране и специално разработени процедури за защита. Чрез тях в потребителите се създава чувство на спокойствие и доверие и това ги превръща в предпочитан способ за извършване на разплащания и опериране с банкови сметки. Това оказва сериозно влияние върху развитието на ЕТ, тъй като пазаруването става по-сигурно и лесно. Потребителите от една страна получават възможност да извършват парични преводи в Интернет, без да въвеждат данните на банковите си карти, както е при приложението CellumPay, а от друга страна, търговците могат да повишават ангажираността на клиентите, като използват тези системи за управление на различни програми за лоялност и отстъпки.

Основни изводи:

1. Проблемите на сигурността в ЕТ са сериозни и многоаспектни. Тяхното решаване се постига с формирането на *последователна стратегия и политика*, които се базират на съвременни бизнес модели. Избраният модел трябва да поддържа шестте измерения на защитените транзакции в ЕТ: *цялостност, неотричане, автентификация, конфиденциалност, неприкосновеност на личните данни и достъпност*.
2. Информационната сигурност в СЕТ се осигурява от две групи решения - *технологични решения и организационни решения*.
3. Технологичните решения включват *криптиране, защитени канали за комуникация, защитени мрежи и защитени сървъри и клиенти*.
4. Политиките за управление на информационната сигурност са насочени към изграждането на план за защита, който цели да се минимизират заплахите за сигурността в СЕТ. Отделните стъпки при разработването на този план включват: *оценка на риска, разработване на политика за сигурност, разработване на план за изпълнение, създаване на организация за сигурността и извършване на одит по сигурността*.
5. *Правните норми и приетите закони* оказват сериозно влияние при функционирането на ЕТ, като гарантират санкции при неправомерни и злонамерени действия. *Индустриалните стандарти* от своя страна определят изискванията, на които трябва да отговаря сигурността на информацията и на технологиите в информационните системи на бизнес организацията.
6. Протоколите за сигурност на информацията намират приложение, както за процедури като удостоверяване и др., така и за подсигуряване на различни частни мрежи като VPN, VoIP мрежи и др. За сигурност в СЕТ основно се използват *протоколи: за удостоверяване; използващи механизми за удостоверяване; за сигурност от различните нива на OSI модела; за сигурност при различни видове частни мрежи*.
7. Ролята и значението на стандартите за информационна сигурност е ключова при осъществяването на бизнес процесите. Сертифицирането на една бизнес организация по световно признат стандарт за информационна сигурност гарантира на клиентите, персонала, управлението и собствениците на компанията, че работната информация е сериозно защитена и системата за управление на тази защита е подходяща и функционираща.

8. Технологиите за защитени електронни разплащания предоставят много сериозно ниво на сигурност на информацията, което се постига чрез криптиране и специално разработени процедури за защита. Тези технологии благоприятстват за масовото използване на мобилни устройства, като правят пазаруването с тях ефективно и безрисково.

Трета глава. Анализ на състоянието и решение за информационна сигурност на електронната търговия в българските организации

Един от ключовите въпроси на организациите в България, които искат да развият успешна електронна търговия, е свързан със сигурността на техните системи за ЕТ и развитието на стратегия за поддържане на информационна безопасност. Защитата на данните е проблем, който често е пренебрегван от българските бизнес организации, за разлика от чуждестранните, където разходите за информационна сигурност са значително по-високи. Емпиричните изследвания на състоянието на информационната сигурност в ЕТ у нас към текущия момент са непълни и засягат отделни нейни аспекти. До сега няма цялостно проучване и анализ на състоянието на информационната сигурност в системите за ЕТ в България.

Като изходна точка за нашето изследване използваме проучване, проведено през 2011 г. и посветено на проблемите на ИТ сигурността в българските организации (Кръстева, ИТ сигурността в българските организации - в дисонанс с глобалните тенденции, 2011). Използваме данни, резултати и изводи от това проучване, за да констатираме настъпили промени, да очертаем евентуални посоки на развитие и да задълбочим изследването в посока на информационната сигурност на СЕТ в българските организации.

3.1. Проблемът със сигурността в българските бизнес организации

Основното заключение от посоченото по-горе проучване от 2011 г. е, че в условията на финансова криза българските бизнес организации избягват сериозни инвестиции, в която и да е област. Поради това техните бюджетите са ограничени, от където следват недостатъчни средства, както за нови технологични решения, така и за квалифициран персонал за информационна сигурност. Най-съществен проблем, въпреки всичко, остава липсата на осведоменост и култура по отношение на проблемите и решенията за информационна сигурност.

По-важните за нас констатации и налагащи се от проучването изводи са в следните насоки:

- *Изоставане в прилагането на редица мерки за сигурност и значително ниски разходи за сигурност на информацията.* Според проучването, през 2011 г. само 12% от организациите в България са увеличили бюджетите си за ИТ сигурност спрямо предходната година. Това е изключително нисък дял, ако сравним със същата стойност, отчетена в световен мащаб (от глобалното проучване на СЮ) – 52%. Според същото изследване, 40% от анкетирания в България заявяват, че бюджетите им за ИТ сигурност остават на нивата от предходната година, когато те са с около 4% по-ниски в сравнение с 2009 г.

Таблица 3.1

Прилагани мерки за ИТ сигурност, %

	% на организациите, в които са приложени	% на организациите, в които са планирани
Сигурно разположение на технологичния хардуер	51%	16%
Активен мониторинг	47%	27%
Стратегия за ИТ сигурност	47%	20%

Наблюдение за спазване на политиката по сигурността	38%	24%
Нива на автентификация, базирани на потребителския риск	36%	16%
Централизиран мениджмънт на информационната сигурност	36%	31%
Стандарти за инфраструктурата	36%	16%
Периодични одити за сигурността	36%	24%
Стандарти за сигурността на портативните устройства	36%	16%
Планове за възстановяване при кризи	31%	24%
Периодични тестове на уязвимостта	27%	16%
Стандарти по сигурността за партньорите	22%	7%
Периодични оценки на риска	22%	31%
Периодични оценки на заплахите и щетите	22%	20%
Програма за обучение на служителите	22%	24%
Стандарти за сигурността на мобилни устройства	22%	16%

Източник: (Кръстева, ИТ сигурността в българските организации - в дисонанс с глобалните тенденции, 2011)

- *Най-популярните мерки за поддържане на някакво ниво на сигурност* са: разполагане на сигурно място на технологичния хардуер, провеждане на активен мониторинг и наблюдение за спазване на политиката за информационна сигурност (таблица 3.1). Не се оценяват достатъчно и са оставени на заден план мерки като: периодични оценки на риска; въвеждане на нива на автентификация, базирани на потребителския риск и др. Най-широко използваните инструменти за ИТ сигурност са: системите за антивирусна защита, потребителските пароли, мрежовите защитни стени (firewalls), системите за резервни копия.

- Сравнително висока активност на *внедряване на решения за централизирано съхранение на данните и VPN софтуер* - с такива инструменти разполагат 51% от анкетираните организации. Наблюдава се също и интерес и към системите, предотвратяващи изтичане на данни - Data Loss Prevention (DLP), като за изследвания период (2010 – 2011) техният дял почти се е удвоил от 6% на 11%.

- По отношение на *бъдещите проекти*, голяма част от анкетираните не посочват какви мерки и технологични инструменти за информационна сигурност се предвижда да бъдат въведени или обновени в техните организации. Причината за това се корени в неясните планове относно бюджетите. От друга страна, в организациите, чиито средства за защита са увеличени спрямо предходната година, проектите се планират доста предпазливо.

- В краткосрочна перспектива компаниите възнамеряват да отдадат по-голямо значение и да отделят повече внимание на *периодичните оценки на риска и на централизираното управление на информационната сигурност*. Заслужено внимание получават и *програмите за обучение* на потребителите. По отношение на технологиите, засилен интерес се наблюдава към системите за наблюдение на потребителската активност, решенията за управление на идентичността и контрола на достъпа и средствата за VoIP сигурност.

• Основните предизвикателства по отношение на информационната сигурност в българските организации включват: *ограничените бюджети, недостатъчният персонал и проблемите във връзка с осведомеността на потребителите* (вж. фиг. 3.1). Недостатъчната информираност по въпросите на ИТ сигурността е фактор, който запазва позицията си в класацията за трите най-големи предизвикателства във връзка с информационната сигурност.



Фиг. 3.1. Предизвикателства пред ИТ сигурността, източник: (Кръстева, ИТ сигурността в българските организации - в дисонанс с глобалните тенденции, 2011)

• В типичния за българските организации случай, на информационната сигурност се гледа като на нещо абстрактно до момента, в който настъпи инцидент. Практиката показва, че броят на организациите, които полагат сериозни усилия за предотвратяване на причините за възникването на инциденти е незначителен. Недостатъчното обучение на потребителите пък води до неразбиране на важността на механизмите за сигурност и поради това се стига до сериозна съпротива срещу тях.

В обобщение можем да заключим, че в условията на финансова криза българските бизнес организации избягват сериозни инвестиции в която и да е област. Поради това бюджетите са ограничени, от където следват недостатъчни средства, както за нови технологични решения, така и за квалифициран персонал за информационна сигурност. Най-съществен проблем въпреки всичко, остава липсата на осведоменост и култура по отношение на информационната сигурност.

3.2. Анализ на състоянието на информационната сигурност в системите за електронна търговия на българските бизнес организации

3.2.1. Аргументиране на избора и описание на методиката на изследване

Изследването², което проведехме, има за цел да допринесе за запълването на празнината относно емпиричните изследвания на състоянието на информационната сигурност в ЕТ в България и да формира база за разработване на модел за политика за сигурност, приложима в българските организации.

Изследването премина през следните етапи:

- планиране на изследването;
- събиране на емпирични данни;
- обобщение, описание и анализ на резултатните данни;
- интерпретация на резултатите – формулиране и проверка на работните хипотези, установяване на функционалните зависимости, оформяне на изводи и заключения.

За събиране на експериментални данни проведехме анкетно проучване. Анкетната карта³, съдържаща 32 въпроса, бе изпратена на 170 бизнес организации с различна големина и сфера на дейност, за чието селектиране беше използван каталога на куриерската фирма Еконт Експрес (Econt, n.d.), представящ онлайн търговците, с които тя има договорени отношения (вж. табл. 3.2).

Получени бяха 36 коректно попълнени анкетни карти, данните, от които са обработени и анализирани със специализирания статистически софтуер SPSS на IBM.

Таблица 3.2

Разпределение на проучените организации по вид на предлаганите стоки/услуги

Вид на предлаганите стоки/услуги	Общ брой организации в раздела на каталога	Брой селектирани организации, на които са изпратени анкетни карти	Респонденти	
			Брой	Относ. дял (%)
Електроника	166	15	1	2.78%
Спорт	66	14	2	5.56%
Книги	22	12	2	5.56%
Мода	221	14	5	13.89%
Автомобили и аксесоари	101	18	3	8.33%
Хипермаркет	13	13	4	11.11%
Мебели	34	6	1	2.78%
Цветя	8	4	1	2.78%
Битова техника	38	19	4	11.11%
Компютри	51	21	3	8.33%
Други	148	35	10	27.78%
ОБЩО:	868	171	36	100%

В модела на анкетата се изследват три групи променливи: номинални, интервални и ординарни, които са под формата на въпроси, на които респондентите трябва да отговорят.

² Изследването беше проведено по проект №13-2013 към Института за научни изследвания, Стопанска академия "Д. А. Ценов" – Свищов - Информационна сигурност в системите за електронна търговия в България, в периода май-юли 2013 г.

³ По-подробно вж. Приложение 1

а) Номиналните променливи са качествени и категорийни и се използват за оценяване и класифициране.

- *Променлива 1: Тип на предприятието*

Целта на тази анкетна единица е да се определи големината на бизнес организацията. Номиналната скала за измерване е дефинирана в Закона за малките и средните предприятия (ЗМСП) в България, показана в табл. 3.3.

Таблица 3.3

Видове предприятия, според ЗМСП⁴

Категория на предприятието	Численост на персонала	Оборот	или	Общ баланс
Средно	>50 и < 250	≤ 97.8 млн. лв.		≤ 84.1 млн. лв.
Малко	>10 и < 50	≤ 19.55 млн. лв.		≤ 15.55 млн. лв.
Микро	< 10	≤ 3.85 млн. лв.		≤ 3.85 млн. лв.

- *Променлива 2: Избран модел на ЕТ.* За оценката на този показател се използва анкетна единица, състояща се от 9 елемента, представящи популярни модели на ЕТ. Аналогично са представят и следващите променливи.

- *Променлива 3: Области на извършване на ЕТ.*

- *Променлива 4: Използвана платформа за ЕТ.*

- *Променлива 5: Сертифициране по стандарта ISO 27001.*

- *Променлива 6: Наличие на инциденти със сигурността през последната година.*

- *Променлива 7: Наличие на екип по сигурността.*

- *Променлива 8: Защитна стена и откриване/предотвратяване на нарушенията.*

- *Променлива 9: Контрол за зловреден софтуер.*

- *Променлива 10: Осъществяване на мониторинг*

б) Интервалните променливи са променливи, за които определени стойности интервали могат да бъдат интерпретирани и съотнасяни. Такива променливи са:

- *Променлива 11: Годишен оборот и стойност на активите.*

- *Променлива 12: Разходи за информационна сигурност.*

- *Променлива 13: Дял от бюджета за ИТ, изразходван за информационна сигурност.*

- *Променлива 14: Среден трудов стаж на персонала, занимаващ се с информационната сигурност.*

в) Ординарните променливи са оценъчни променливи, които могат да се сравняват, но не и да се съотнасят. На тяхна база се осъществява наблюдение, което предоставя отговори на набор от предварително зададени категории. По този начин се създават равни общи условия за наблюдение, при които ординарната скала (ранговете) се подреждат в определен ред, като точки за измерване и се създават условия за измерване на качествени критерии. Целта е различни фактори и критерии да се представят като ординарни променливи, които могат да бъдат измерени.

- *Променлива 15: Приоритет на информационната сигурност.* За оценката на този показател се използва анкетна единица с 4 елемента (много висок приоритет, висок приоритет, нисък приоритет, не е приоритет).

⁴ Данните в ЗМСП са представени в лева, съгласно курса на еврото спрямо БНБ - 1.95583 лв. за 1 евро.

- *Променлива 16: Разработени политики и процедури за сигурност.* За оценката на този показател се използва анкетна единица, състояща се от 9 елемента, като всеки визиращ различни аспекти, които сме определили като особено важни в защитната политика.

- *Променлива 17: Степента на конфиденциалност на данните, с които се работи през Интернет.*

- *Променлива 18: Главната причина за направените от организацията разходи за информационна сигурност.* За оценката на този показател се използва анкетна единица, състояща се от 10 елемента, като всеки визиращ различни аспекти, които са определени като особено показателни.

- *Променлива 19: Начини за измерване на ефективността на разходите за информационна сигурност*

- *Променлива 20: Тип на инцидентите със сигурността.*

- *Променлива 21: Тип на физически контрол на достъпа до данните.*

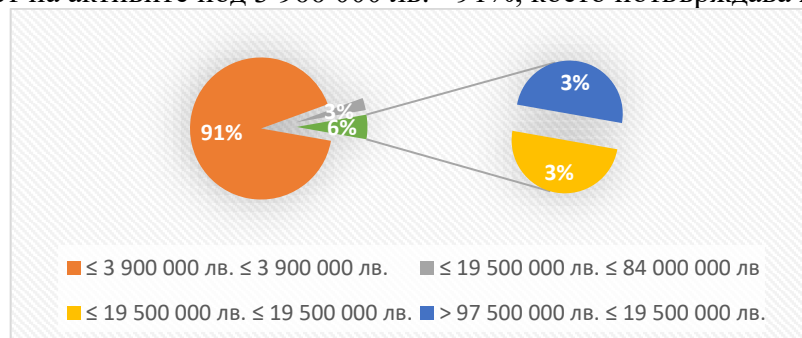
3.2.2. Основни резултати от проучването

За обобщение, описание и анализ на резултатните данни използваме: дескриптивна статистика - за описание на получените резултати; χ^2 тест – за проверка на хипотези; корелация, линейна или нелинейна регресия – за установяване на функционални зависимости.

Първата група от въпроси в анкетата имат за цел да се добие базова информация за изследваните бизнес организации.

Изследователската хипотеза предполага основната част от респондентите да са микро и малки организации, тъй като частта на последните е най-многобройна от селектираните. Отчетените резултати потвърждават хипотезата и показват, че преобладаващата част от бизнес организациите, според ЗМСП попадат в групата на микро (81%) и малките (14%) предприятия. Това предполага ограничени ресурси за поддържане на собствен ИТ персонал, собствена ИТ инфраструктура и отделяне на достатъчно средства за информационна сигурност.

По отношение на **годишния оборот и стойността на активите**, 3% са отговорили, че имат по-малко от 19 500 000 лв. годишен оборот и стойност на активите под 19 500 000 лв., 3% са посочили - съответно 19 500 000 лв. и 84 000 000 лв. Само 3 % са посочили, че оборотът им е над 97 000 000 лв., а най-висок е процента на тези с годишен оборот и стойност на активите под 3 900 000 лв. - 91%, което потвърждава хипотезата.



Фиг.3.2. Годишен оборот и стойност на активите

От получените данни можем да направим извода, че преобладаващата част от организациите, осъществяващи ЕТ, според ЗМСП попадат в групата на малките (14%)

предприятия и микро (81%). Това предполага ограничени ресурси за поддържане на собствен ИТ персонал, собствена ИТ инфраструктура и отделяне на достатъчно средства за информационна сигурност.

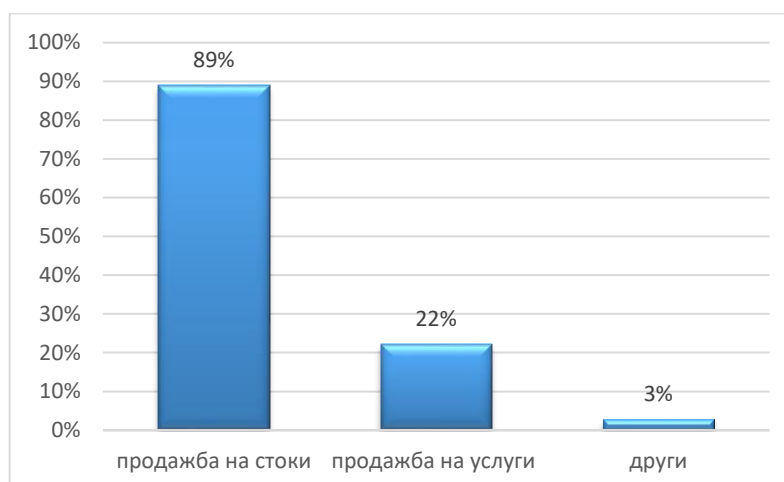
Относно **избрания модел на ЕТ**, изследователската хипотеза предполага най-голям дял за електронен магазин, тъй като това е най-разпространеният модел в страната. Най-малък е дялът на електронен МОЛ – 3%, доставчици на услуги с добавена стойност – 3% и платформи за сътрудничество – 3%. След тях се нареждат електронни търгове с 8%, а 86% от респондентите са посочили електронен магазин, което потвърждава хипотезата



Фиг. 3.3. Избран модел на ЕТ

Масово използваната форма за ЕТ е електронен магазин – 86%, сравнително малко (само 3%) са организациите, предлагащи услуги на търговците и другите участници в ЕТ. Взимайки предвид тенденцията за увеличаване предлагането и използването на услуги, като изчисления в облака и др., очакваме дялът на тези организации да нараства. Сравнително висок е дялът на бизнес организациите, предлагащи електронни търгове. Електронните търгове са форма на ЕТ, която получава все по-голямо разпространение и позволява като търговци да участват и физически лица.

По отношение на **областите на извършване на ЕТ**, основната хипотеза гласи, че продажбата на стоки ще бъде областта с най-голям дял, поради слабото развитие на останалите. 3% от респондентите са посочили други, 22% са посочили продажба на услуги, а 89% са посочили продажба на стоки и това потвърждава хипотезата. Прави впечатление, че процентите от отговорите надхвърлят 100. Това е така, понеже част от организациите са посочили по-вече от един отговор. Същото важи и за подобни въпроси, където процентите надвишават 100.

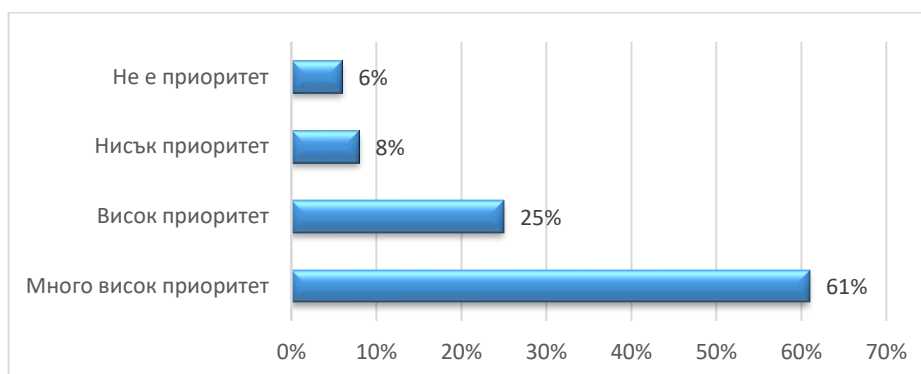


Фиг. 3.4. Област на извършване на ЕТ

ЕТ в изследваните организации е насочена преобладаващо към продажбата на стоки – 89%, само 22% се занимават с продажба на услуги. Онлайн продажбата на услуги е едно направление в ЕТ, което се очаква да получи значително развитие в бъдеще.

Втората група въпроси в анкетата имат за цел да се изследват стратегиите и процедурите за сигурност и контрол.

По отношение **приоритета на информационната сигурност** за изследваните организации, основната хипотезата предполага той да е много висок, поради важността на информацията, с която се оперира. За 6% от респондентите информационната сигурност не е приоритет, за 8% тя е с нисък приоритет, 25% я определят с висок приоритет, а отчетените 61% от респондентите, които са посочили, че информационната сигурност е с много висок приоритет за тях, потвърждават хипотезата. Високите стойности на този показател (61% - много висок, 25% - висок) са очаквани, като се има предвид, че организациите, извършващи ЕТ, събират и съхраняват лични данни за клиентите си (вж. фиг. 3.5).



Фиг. 3.5. Приоритет на информационната сигурност за изследваните организации.

Обобщавайки можем да направим извода, че изследваните организации определят приоритета на информационната сигурност като висок или много висок. Това е очаквано, като се има предвид, че компаниите извършват онлайн бизнес.

На въпроса относно **разработените в организацията политики и процедури** (вж. фиг. 3.6), изследователската хипотеза предполага политиките за управление на данните и за криптиране да са с висок дял. Резултатите показват, че в разглеждания контекст

28% посочват „политика за управление на данните (която да включва използване на данните, съхраняване и унищожаване на чувствителни данни)“ и това опровергава хипотезата. Ситуацията е сходна и в проведеното проучване на СЮ през 2011 г., където този процент е 38. Останалата част от респондентите в проучването ни са посочили „политика и стандарти на криптиране“ – 31%, „отговор и управление на инциденти, свързани със сигурността“ – 33%, „отдалечен достъп до мрежата на организацията“ – 33%, „придобиване на софтуер и хардуер“ – 39% , „управление на паролите“ – 42%, „оторизиране използването на мрежови услуги“ – 47%, „използване на корпоративния e-mail, интранет и Интернет“ – 47% и „практиките на персонала“ са посочени от 61% и са с най-голям дял.

Трябва да се отбележи важното място, което заемат практиките на персонала в политиката и стратегията на организацията (61%). Това показва доверието, което ръководителите на организациите имат в ИТ персонала, ангажиран в информационната сигурност чрез аутсорсинг или в собствения ИТ персонал.

По-малко значение се отдава на технологиите за управление на данните (само 28% от респондентите ги прилагат). Тук се наблюдава значителен потенциал за усъвършенстване на политиката и стратегиите за изграждане и поддържане на информационна сигурност, тъй като политиката за управление на данните трябва да бъде основополагаща в стратегията за информационна сигурност. Тя може да се поддържа с организационни и технологични средства.



Фиг. 3.6. Разработени политики и процедури за сигурност в изследваните организации.

От представените данни можем да направим извода, че в политиката и стратегията за информационна сигурност организациите разчитат предимно на практиките на персонала, а най-малко значение отделят на политиката за управление на данните, въпреки че работят с лични и конфиденциални данни.

По отношение на степента на **конфиденциалност на данните**, с които се работи през Интернет, изследователската хипотеза предполага данните да са високо конфиденциални и тя се потвърждава с 42% от респондентите, които определят данните си като високо конфиденциални и 44% от респондентите, за които данните са конфиденциални, докато за останалите 14% данните не са конфиденциални.

Бизнес организациите добре разбират значението на управляваните от тях данни. За 86% данните са високо конфиденциални или конфиденциални. Това е обстоятелство, което също налага да бъде отделено необходимото внимание на политиката за управление на данните.

Прави впечатление, че само една от организациите е **сертифицирана по стандарт ISO 27001**. От останалите 35 респондента, само 3 планират сертифициране през следващите 12 месеца.

Относно използваната **платформа за ЕТ**, изследователската хипотеза предполага платформата да е разположена на външен сървър, поради ограничените финансови възможности на организациите. Резултатите показват, че 12 от изследваните организации посочват, че платформата им е разположена на собствен сървър, администриран от персонала на организацията. Останалите 24 респондента използват платформа за ЕТ, хоствана от доставчик на Интернет услуги.

Предвид преобладаващата част на малките и микро предприятия (общо 95%), нашата хипотеза за използване на платформи на доставчици на услуги и осигуряване на информационната сигурност чрез аутсорсинг се потвърждава в по-голямата си част. Само 33% поддържат собствена инфраструктура, администрирана от собствен ИТ персонал. За останалите 67% информационната сигурност на електронния магазин се и поддържа от външни доставчици на услуги.

Следващата група въпроси имат отношение към инвестициите в информационна сигурност.

На въпроса **коя е главната причина за направените разходи за информационна сигурност**, изследователската хипотеза предполага главните причини да включват защита от кражба и предотвратяване на престопите и прекъсванията. Според проучването ни 8% посочват поддържане на бизнеса в ситуация на бедствие, 11% – други, 17% – предоставяне на нови бизнес възможности, 19% – поддръжка на интеграцията на данните, 28% – предотвратяване на престопите и прекъсванията, 31% – защита на интелектуалната собственост, 39% посочват защита на различните активи от кражба, 42% – защита на репутацията на организацията, 50% – придържане към законите и разпоредбите и 53% – повишаване на ефективността (вж. фиг. 3.7).



Фиг. 3.7. Причини за направените разходи за информационна сигурност.

Когато се правят разходи за информационна сигурност в българските организации, развиващи ЕТ, първите три приоритета са повишаване на ефективността, придържане към законите и наредбите и защита репутацията на организацията, което опровергава хипотезата ни. За сравнение със световните тенденции, според проведеното от компанията PwC изследване (PwC, 2013), през 2013 г., това са икономическите условия (41.59%), поддържане непрекъснатостта на бизнеса/предпазване от сривове – 30.26% и репутацията на компанията – 30.22%. Прави впечатление, че кражбата на информация не е сред водещите причини за разходите за информационна сигурност, докато според нашето изследване тя е важна причина за 39% от организациите, а според цитираното изследване е причина само за 16.67% от компаниите.



Фиг. 3.8. Разходи за информационна сигурност

Относно относителния дял от бюджета на организацията, който се използва за информационна сигурност, изследователската хипотеза предполага делът на бюджета за информационна сигурност да е около 5% поради ограничените финансови възможности на българските бизнес организации. Според проучването ни, за 2,86% от респондентите разходите са 11% и 25% от бюджета за ИТ, 17,14% посочват, че са отделили 1% или по-малко от бюджета за ИТ, за 17,14% тези разходи са между 6% и 10% от бюджета, 22,86% от респондентите са отговорили, че нямат разходи за информационна сигурност, а 40% са похарчили за информационна сигурност между 2% и 5% от бюджета си (вж. фиг. 3.8). Констатираните 40%, които са похарчили между 2% и 5% от бюджета си, потвърждават хипотезата.

Въпреки че, информационната сигурност има висок приоритет след изследваните организации (61% заявяват, че за тях приоритетът е много висок и 25% го определят като висок), притеснение будят фактите, че 22,86% от анкетираните нямат никакви разходи за информационна сигурност, а други 17,14% правят много малки разходи (1% от бюджета за ИТ). За сравнение със световните тенденции ще посочим, че според изследване на Gartner, проведено през 2010 г. (Carlson, 2010), компаниите изразходват средно 5% от ИТ бюджета за информационна сигурност. Липсата на разходи или ограниченият им размер може да обясним с особеностите на изследваните организации. Те са предимно микро- и малки предприятия, използващи чужда инфраструктура, която се администрира и поддържа от персонала на доставчика на услугата. За осигуряване собствената информационна сигурност се използват предимно безплатни софтуерни продукти (антивирусни програми, защитни стени и др.). Въпреки че сред безплатните софтуерни продукти, поддържащи информационната сигурност, съществуват и такива, които са с много добри възможности, те не покриват пълната функционалност на комерсиалните продукти.

Четвъртата група въпроси, включени в анкетата имат отношение към **нарушенията в сигурността**. Хипотезата за тази област предполага пробивите в сигурността да са често срещано явление предвид факта, че основната част от селектираните организации са малки и микро и сайтовете им не са добре функциониращи и не разполагат със сериозни технологии за защита.

Учудване буди фактът, че 78% от респондентите посочват в анкетните си карти, че през последната година не са регистрирали пробив в сигурността и този резултат опровергава хипотезата ни. От останалата част на респондентите, 6% от анкетираните са имали случаен инцидент, само 6% са имали злонамерен инцидент и 11% са имали някакъв инцидент в сигурността. За сравнение с проведеното световно проучване на PwC, без инциденти са само 20.48% от компаниите, а 31.38% декларират между 1 и 9 инцидента на година. Световната практика показва, че от нарушения в сигурността страдат повече големите компании – 93%, докато при малките компании тя е 87% (PwC, 2013 Information security breaches survey, 2013).

Липсата на инциденти със сигурността, заявена от повече от три четвърти от организациите (78%) се разминава съществено със световните тенденции на увеличаване на заплахите, според които този брой е едва една пета (20.5%). Състоянието у нас можем да обясним с няколко причини: вида на бизнеса, който е малък и не представлява интерес за нарушителите; липсата на информация за извършени нарушения в сигурността; нежелание да бъде споделена информация за пробиви в сигурността.

Следващата група въпроси се отнася до организиране на физическата сигурност в компаниите. Нашата хипотезата предполага строг контрол на достъпа до централите с

данни. Най-важната констатация е, че само 55% от респондентите посочват, че извършват наблюдение и записване на действията, свързани с достъп до центъра с данни и това отчасти потвърждава предположенията ни.

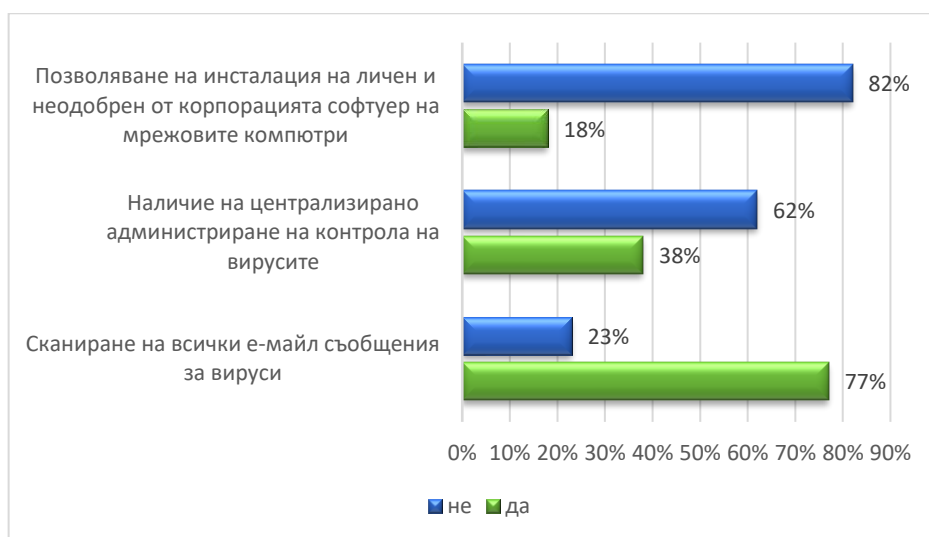
Шестата група въпроси засяга администрирането на сигурността на информацията. Изследователската хипотеза предполага сериозно отношение към този проблем и наличие на адекватно администриране. Но на въпроса дали са дефинирани ограничения в нивата на достъп на администраторите на мрежовата и системната инфраструктури до системата, само 36% от респондентите отговарят положително, което опровергава нашата хипотеза.

Седмата група въпроси са ориентирани към организирането на защитата, използваната защитна стена и откриване/предотвратяване на нарушенията. Хипотезата за тази група предполага засилени мерки за справяне с пробивите в сигурността и масово използване на защитна стена. По отношение на наличието на екип по сигурността, който да следи за известните заплахи, 49% от респондентите посочват, че имат такъв екип, а 69% имат екип, който реагира само при констатиране на инцидент. Защитна стена използват 68% от респондентите (вж. фиг. 3.9), 58% сканират и проверяват всички допустими услуги, предоставяни от сървъра на защитната стена и 63% имат инструменти за отчитане и анализиране на дневниците (log) на защитната стена. Относно наличието на документирана и проверена политика за сигурност на защитната стена, 42% посочват, че разполагат с такава. С констатираните резултати можем да отбележим, че нашата хипотеза отчасти се потвърждава.



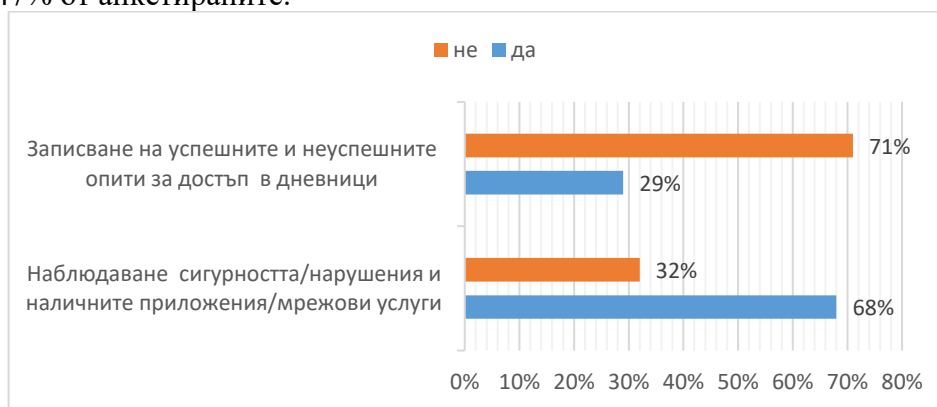
Фиг. 3.9. Използване на защитна стена

Следващата група въпроси се отнася до осъществяването на контрол върху зловредния софтуер. Изследователската хипотеза предполага сериозно внимание и контролиране на зловредния софтуер и тя се потвърждава с отговорите на повече от три четвърти (77%) от респондентите, които заявяват, че сканират за вируси всички e-mail съобщения и голяма част (82%), които не позволяват инсталация на личен или неодобрен от корпорацията софтуер върху мрежови компютри. Само 13% имат централизирано администриране на контрола за вируси (вж. фиг. 3.10).



Фиг. 3.10. Сканиране на всички входящи имейли за вируси

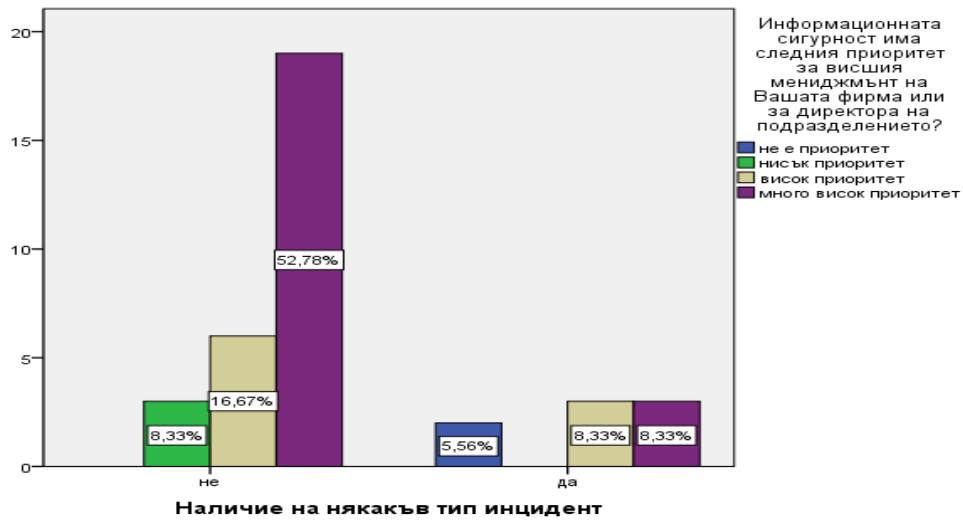
Последната група въпроси е относно осъществяването на мониторинг на мрежовите услуги. Хипотезата ни предполага сериозно отношение и отчетност на опитите за нарушения на сигурността. Констатациите са, че само 29% регистрират в дневници успешните и неуспешните опити за достъп, което отчасти потвърждава хипотезата, а наблюдения върху сигурността / нарушения и наличните приложения / мрежови услуги извършват повече от две трети (68%) от анкетиранияте, (вж. фиг. 3.11). За сравнение, проучването за българските бизнес организации за 2011 г. отчита, че активен мониторинг извършват 47% от анкетиранияте.



Фиг. 3.11. Наблюдение на сигурността и нарушенията и наличните мрежови услуги

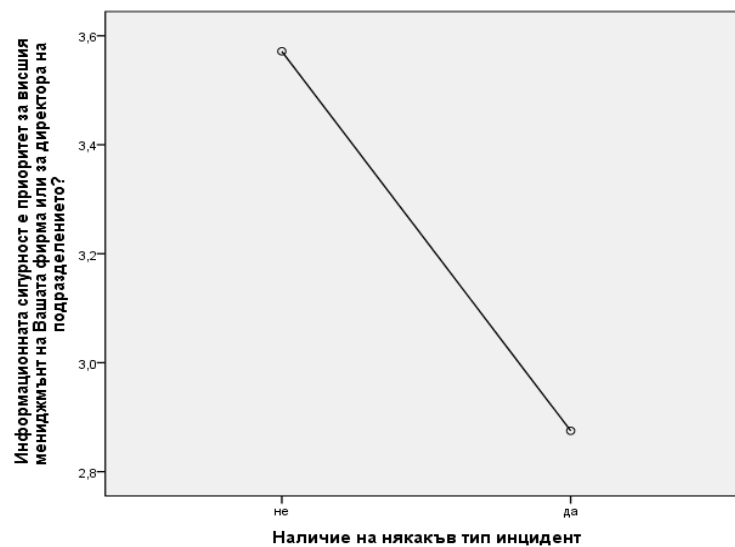
При анализа на данните бяха съставени множество кростаблици за изследване на съвместното вероятностно разпределение на две категорийни променливи, като основната цел е откриване на връзки или липсата на връзки между неметричните променливи. Основната идея е задълбоченото статистическо изучаване на тези връзки с помощта на статистически тестове за доказване на тяхното наличие и сила. Основният статистически тест, който използваме за проверка на хипотезата за наличието на връзка между две неметрични променливи, е т.нар. χ^2 **тест за независимост**, който се основава на очакваната стойност на всяка клетка от кростаблицата, като се приема, че не съществува връзка между променливата по редовете и променливата по колоните.

Първите две променливи, за които се извърши проверка за съществуване на връзка са *наличие на инцидент* и *приоритет на информационната сигурност*.



Фиг. 3.12. Връзка между приоритет на информационната сигурност и наличие на инцидент

Връзката е представена в графичен вид на фиг. 3.13., където се вижда обратната зависимост между променливите.



Фиг. 3.13. Връзка между приоритет на информационната сигурност и наличие на инцидент

Таблица 3.4

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	9.438 ^a	3	.024
Likelihood Ratio	9.156	3	.027
Linear-by-Linear Association	3.949	1	.047
N of Valid Cases	36		

a. 6 cells (75.0%) have expected count less than 5. The minimum expected count is .44.

Най-популярна е първата стойност на χ^2 теста, която носи името на **Карл Пирсън** (Кръстевич, 2010). Нулевата хипотеза при χ^2 теста гласи, че в генералната съвкупност няма връзка между променливите, което може да се опровергае при наличие на емпирично равнище на значимост по-малко 0,05, което свидетелства за значимост на теста и може да се направи извод, че между дадени две променливи съществува статистически значима връзка.

В случая стойността е 0,0239967575311472 - по-малко от критичното 0,05, следователно налице е статистически значима връзка между променливите.

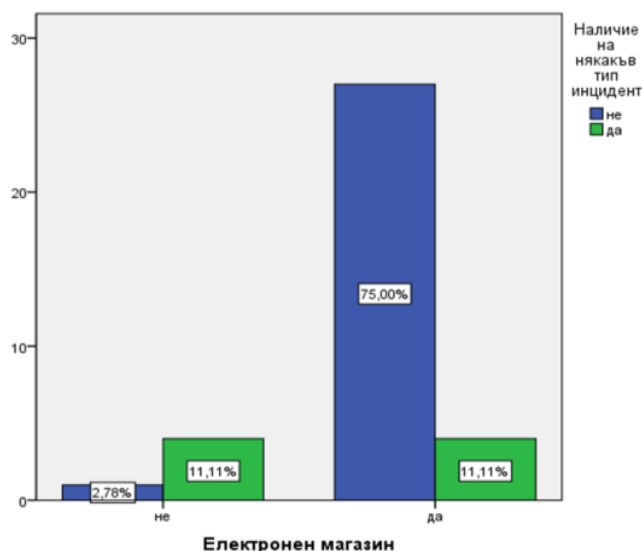
Трябва да се отбележи, че с използването на χ^2 теста се показва до колко е вероятно наличието на връзка между анализиранияте променливи, но не изразява по никакъв начин посоката на и/или интензивността на тази връзка. Силата и интензивността на връзката се определят чрез коефициента **Ламбда** и коефициента **тау** на **Гудман и Кръскал** (Кръстевич, 2010). Тези коефициенти приемат стойности между 0 и 1 в зависимост от силата на връзката.

Таблица 3.5

		Value	Asymp. Std. Error ^a	Approx. T ^b	Approx. Sig.	Exact Sig.
Lambda	Symmetric	.091	.120	.712	.476	
	Наличие на някакъв тип инцидент Dependent	.250	.153	1.455	.146	
	Информационната сигурност има следния приоритет за висшия мениджмънт на Вашата фирма или за директора на подразделението? Dependent	0,000	.175	0,000	1,000	
Goodman and Kruskal tau	Наличие на някакъв тип инцидент Dependent	.262	.084		.027 ^c	.028
	Информационната сигурност има следния приоритет за висшия мениджмънт на Вашата фирма или за директора на подразделението? Dependent	.060	.057		.098 ^c	.118
Uncertainty Coefficient	Symmetric	.165	.076	1.919	.027 ^d	.038
	Наличие на някакъв тип инцидент Dependent	.240	.120	1.919	.027 ^d	.038
	Информационната сигурност има следния приоритет за висшия мениджмънт на Вашата фирма или за директора на подразделението? Dependent	.125	.057	1.919	.027 ^d	.038

В случая при допускане, че приоритетът на информационната сигурност влияе върху наличието на инцидент, се интерпретира стойността на ламбда в етикет "Наличие на инцидент" Dependent. Стойността е 0.250, което показва сравнително силна интензивност на връзката между променливите.

Интерес буди и връзката между променливите *електронен магазин* и *наличие на инцидент*, тъй като най-използваният модел за ЕТ е електронният магазин.



Фиг. 3.14. Връзка между електронен магазин и наличие на инцидент

Таблица 3.6

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	11,215 ^a	1	,001		
Continuity Correction ^b	7,669	1	,006		
Likelihood Ratio	9,293	1	,002		
Fisher's Exact Test				,005	,005
Linear-by-Linear Association	10,903	1	,001		
N of Valid Cases	36				

a. 2 cells (50,0%) have expected count less than 5. The minimum expected count is 1,11.

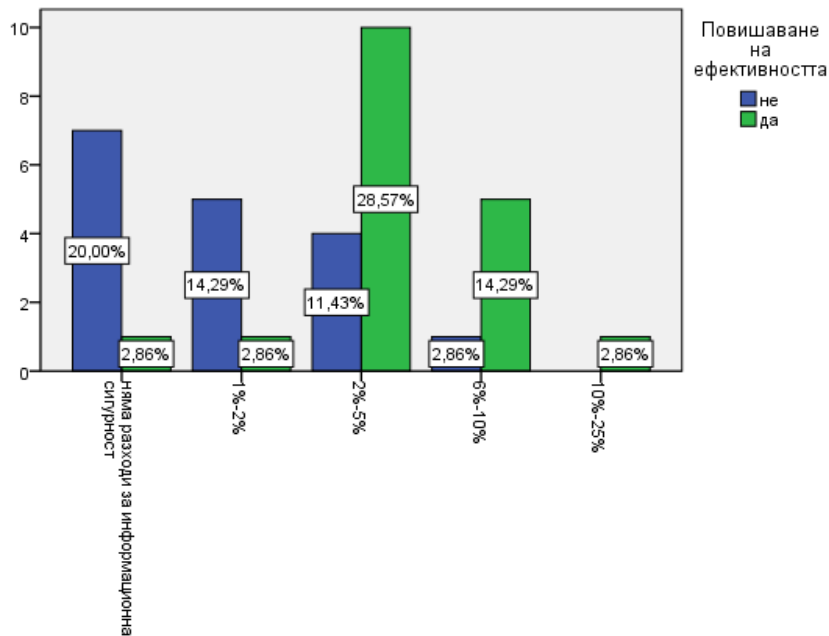
b. Computed only for a 2x2 table

При изследването на тази връзка, стойността на χ^2 теста е 0,000811498922036037, много под критичното и следователно между променливите съществува статистически значима връзка. Коефициентът ламбда в етикет "Наличие на тип инцидент" Dependent със стойност 0.375 показва, че откритата връзка е със силна интензивност.

Таблица 3.7

			Value	Asymp. Std. Error ^a	Approx. T ^b	Approx. Sig.
Nominal by Nominal	Lambda	Symmetric	,231	,318	,659	,510
		Електронен магазин Dependent	0,000	,566	0,000	1,000
		Наличие на някакъв тип инцидент Dependent	,375	,221	1,376	,169
	Goodman and Kruskal tau	Електронен магазин Dependent	,312	,191		,001 ^c
		Наличие на някакъв тип инцидент Dependent	,312	,178		,001 ^c
	Uncertainty Coefficient	Symmetric	,277	,166	1,521	,002 ^d
		Електронен магазин Dependent	,320	,184	1,521	,002 ^d
		Наличие на някакъв тип инцидент Dependent	,244	,155	1,521	,002 ^d

Следващата двойка променливи, за които се извърши статистически тест, са *част от бюджета, използвана за информационна сигурност и повишаване на ефективността*, като цел за направените разходи.



Каква част от бюджета за ИТ се изразходва за информационна сигурност?

Фиг. 3.15. Връзка между част от бюджета, изразходвана за информационна сигурност и повишаване на ефективността, като цел за извършените разходи.

Таблица 3.8

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	13,387 ^a	4	,010
Likelihood Ratio	14,898	4	,005
Linear-by-Linear Association	11,505	1	,001
N of Valid Cases	35		

a. 8 cells (80,0%) have expected count less than 5. The minimum expected count is ,49.

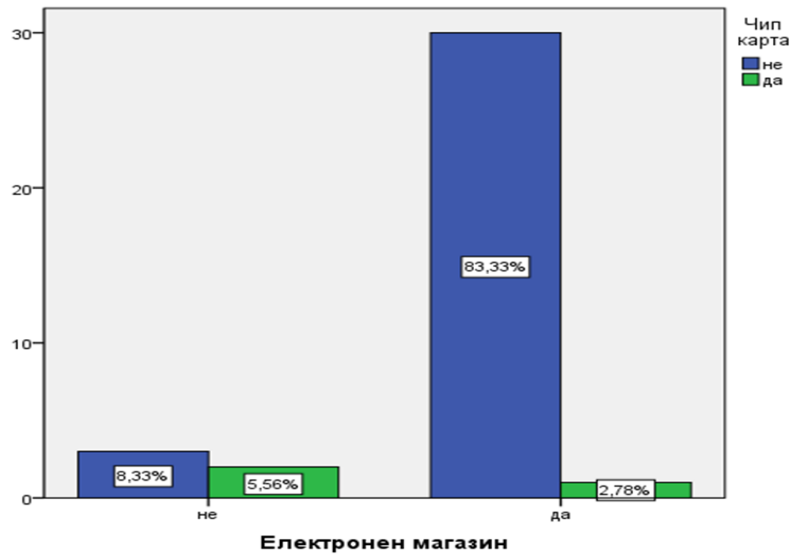
Стойността на Карл Пирсън теста е 0,00953128402792991, също е по-ниска от критичната 0,05 и това дава основание да се направи изводът, че между променливите съществува статистически значима връзка. Стойността на коефициента ламбда- 0.588 в етикет „Повишаване на ефективността“ Dependent показва, че направените разходи за информационна сигурност влияят върху повишаването на ефективността като цел за направените разходи и връзката е силно интензивна.

Таблица 3.9

			Value	Asymp. Std. Error ^a	Approx. T ^b	Approx. Sig.
Nominal by Nominal	Lambda	Symmetric	,342	,131	2,224	,026
		Каква част от бюджета за ИТ се изразходва за информационна сигурност? Dependent	,143	,146	,915	,360
		Повишаване на ефективността Dependent	,588	,141	2,996	,003
	Goodman and Kruskal tau	Каква част от бюджета за ИТ се изразходва за информационна сигурност? Dependent	,116	,056		,003 ^c
		Повишаване на ефективността Dependent	,382	,151		,011 ^c
	Uncertainty Coefficient	Symmetric	,202	,087	2,296	,005 ^d
Каква част от бюджета за ИТ се изразходва за информационна сигурност? Dependent		,151	,064	2,296	,005 ^d	
Повишаване на ефективността Dependent		,307	,134	2,296	,005 ^d	

Следващият статистически тест обвързва променливите *електронен магазин като модел за ЕТ и използване на чип карта като способ за контрол на периметъра за достъп до данните*.

Стойността на χ^2 теста е 0,00576513185526296, много под критичното, следователно между променливите съществува значима връзка.



Фиг. 3.16. Връзка между електронен магазин и използване на чип карта като способ за контрол на периметъра за достъп до данни.

Таблица 3.10

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	7,622 ^a	1	,006		
Continuity Correction ^b	3,568	1	,059		
Likelihood Ratio	5,087	1	,024		
Fisher's Exact Test				,045	,045
Linear-by-Linear Association	7,411	1	,006		
N of Valid Cases	36				

a. 3 cells (75,0%) have expected count less than 5. The minimum expected count is ,42.

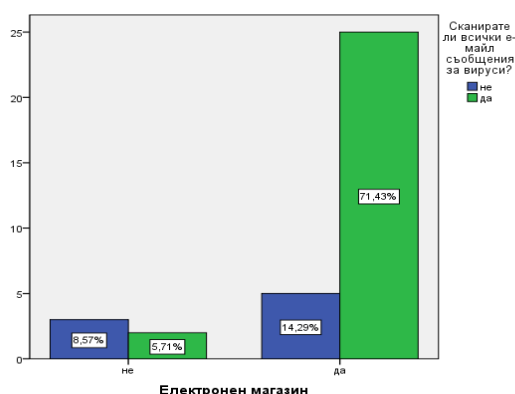
b. Computed only for a 2x2 table

Коефициентът ламбда със стойност 0 не показва интензивност на връзката, затова се насочваме към коефициента на Гудман и Кръскал, стойността на който е 0,212 и показва сравнително силна интензивност на връзката.

Таблица 3.11

			Value	Asymp. Std. Error ^a	Approx T ^b	Approx Sig.
Nominal by Nominal	Lambda	Symmetric	,125	,195	,580	,562
		Електронен магазин Dependent	,200	,310	,580	,562
		Чип карта Dependent	0,000	0,000	^c	^c
	Goodman and Kruskal tau	Електронен магазин Dependent	,212	,196		,006 ^d
		Чип карта Dependent	,212	,207		,006 ^d
		Uncertainty Coefficient	Symmetric	,205	,184	1,016
	Uncertainty Coefficient	Електронен магазин Dependent	,175	,165	1,016	,024 ^e
		Чип карта Dependent	,246	,214	1,016	,024 ^e

Следващите променливи, над които се извърши статистически тест, са *електронен магазин*, като използван модел за *ЕТ* и *сканиране на всички имейли*, като техника за повишаване на *информационната сигурност*.



Фиг. 3.17. Връзка между електронен магазин и сканиране на всички е-мейл съобщения

Таблица 3.12

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	4,564 ^a	1	,033		
Continuity Correction ^b	2,437	1	,118		
Likelihood Ratio	3,864	1	,049		
Fisher's Exact Test				,067	,067
Linear-by-Linear Association	4,434	1	,035		
N of Valid Cases	35				

a. 2 cells (50,0%) have expected count less than 5. The minimum expected count is 1,14.

b. Computed only for a 2x2 table

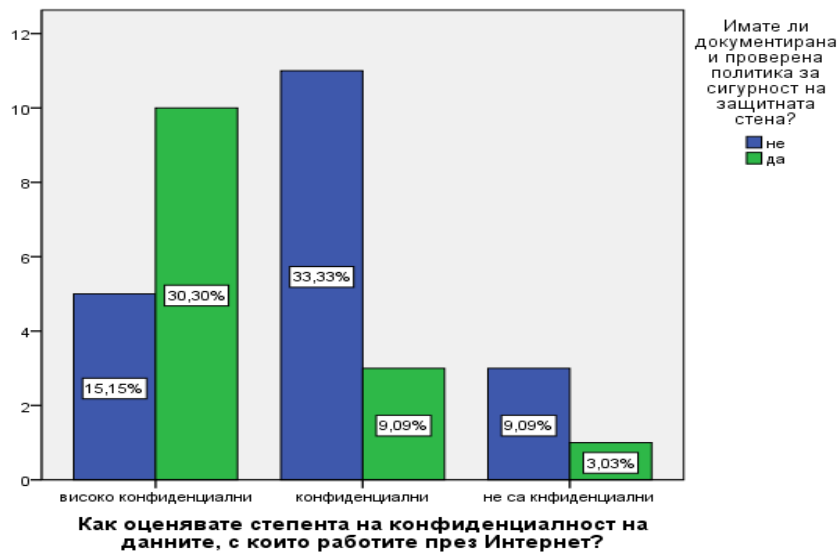
Стойността на χ^2 теста тук е 0,0326499071731877 и също е под критичното ниво, следователно между променливите съществува връзка.

Таблица 3.13

			Value	Asymp. Std. Error ^a	Approx. T ^b	Approx. Sig.
Nominal by Nominal	Lambda	Symmetric	,077	,163	,448	,654
		Електронен магазин Dependent	0,000	0,000	.	.
		Сканирате ли всички е-мейл съобщения за вируси? Dependent	,125	,261	,448	,654
	Goodman and Kruskal tau	Електронен магазин Dependent	,130	,139		,035 ^d
		Сканирате ли всички е-мейл съобщения за вируси? Dependent	,130	,136		,035 ^d

Коефициентът ламбда в етикета "Сканирате ли всички е-мейл съобщения за вируси?" Dependent е със стойност 0,125 и ни дава основание да твърдим, че връзката между променливите е сравнително силно интензивна.

Следващата двойка променливи са как оценявате степента на конфиденциалност на данните и наличие на документирана и проверена политика за сигурност на защитната стена.



Фиг. 3.18. Връзка между оценката за конфиденциалност на данните и наличие на документирана и проверена политика за сигурност на защитната стена

Таблица 3.14

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	6,633 ^a	2	,036
Likelihood Ratio	6,845	2	,033
Linear-by-Linear Association	4,862	1	,027
N of Valid Cases	33		

a. 2 cells (33,3%) have expected count less than 5. The minimum expected count is 1,70.

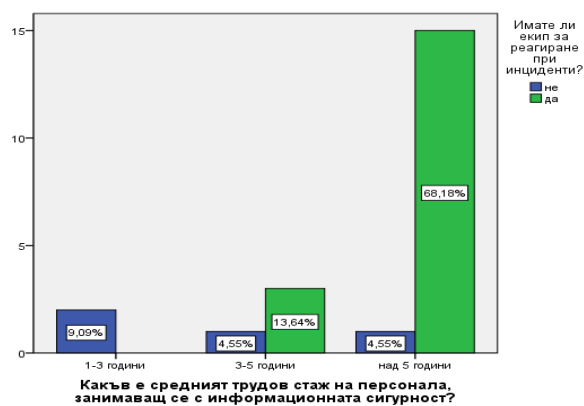
Стойността на χ^2 теста - 0,0362834464374199 е под критичното, което свидетелства за наличието на връзка между променливите.

Таблица 3.15

			Value	Asymp. Std. Error ^a	Approx. T ^b	Approx. Sig.
Nominal by Nominal	Lambda	Symmetric	,344	,175	1,800	,072
		Как оценявате степента на конфиденциалност на данните, с които работите през Интернет? Dependent	,333	,181	1,554	,120
	Имате ли документирана и проверена политика за сигурност на защитната стена? Dependent	,357	,222	1,325	,185	
	Goodman and Kruskal tau	Как оценявате степента на конфиденциалност на данните, с които работите през Интернет? Dependent	,140	,100		,011 ^c
Имате ли документирана и проверена политика за сигурност на защитната стена? Dependent		,201	,140		,040 ^c	

Стойността на коефициента ламбда в етикет „Имате ли документирана и проверена политика за сигурност на защитната стена? Dependent“ - 0.357 показва, че връзката е силно интензивна.

Следващият статистически тест включва променливите *среден трудов стаж на персонала, занимаващ се с информационна сигурност* и *наличие на екип за реагиране при инциденти*.



Фиг. 3.19. Връзка между среден трудов стаж на персонала, занимаващ се с информационна сигурност и наличие на екип за реагиране при инциденти

Таблица 3.16

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	10,656 ^a	2	,005
Likelihood Ratio	8,882	2	,012
Linear-by-Linear Association	8,872	1	,003
N of Valid Cases	22		

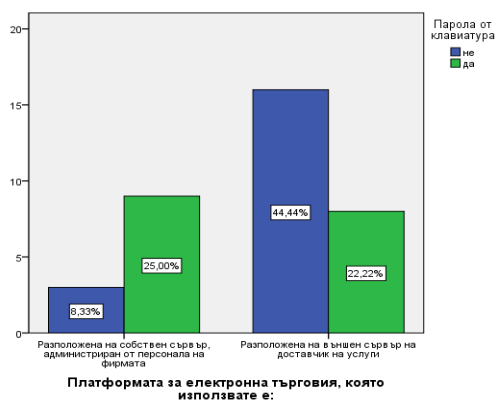
a. 5 cells (83,3%) have expected count less than 5. The minimum expected count is ,36.

Стойността на χ^2 теста е 0,00485316116381311, който е много под критичното ниво и показва, че съществува връзка между променливите и тази връзка е силно интензивна, понеже коефициентът ламбда в етикет „Имате ли екип за реагиране при инциденти?“ Dependent е 0.5.

Таблица 3.17

			Value	Asymp. Std. Error ^a	Approx. T ^b	Approx. Sig.
Nominal by Nominal	Lambda	Symmetric	,300	,250	1,024	,306
		Какъв е средният трудов стаж на персонала, занимаващ се с информационната сигурност? Dependent	,167	,264	,582	,561
		Имате ли екип за реагиране при инциденти? Dependent	,500	,250	1,483	,138
	Goodman and Kruskal tau	Какъв е средният трудов стаж на персонала, занимаващ се с информационната сигурност? Dependent	,207	,153		,013 ^c
		Имате ли екип за реагиране при инциденти? Dependent	,484	,168		,006 ^c
	Uncertainty Coefficient	Symmetric	,327	,159	1,748	,012 ^d
Какъв е средният трудов стаж на персонала, занимаващ се с информационната сигурност? Dependent		,266	,128	1,748	,012 ^d	
Имате ли екип за реагиране при инциденти? Dependent		,426	,223	1,748	,012 ^d	

Последната двойка променливи са *разположение на платформата за електронна търговия и пароли от клавиатура като тип контрол на периметъра за достъп до данните.*



Фиг.3.20. Връзка между разположението на платформата за ЕТ и парола от клавиатурата като контрол на периметъра

Таблица 3.18

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	5,573 ^a	1	,018		
Continuity Correction ^b	4,026	1	,045		
Likelihood Ratio	5,747	1	,017		
Fisher's Exact Test				,033	,022
Linear-by-Linear Association	5,418	1	,020		
N of Valid Cases	36				

a. 0 cells (,0%) have expected count less than 5. The minimum expected count is 5,67.

b. Computed only for a 2x2 table

Стойността на теста на Карл Пирсън е 0,0182420326556942. Получената стойност е под критичната 0,05 и показва, че между променливите съществува връзка.

Таблица 3.19

			Value	Asymp. Std. Error ^a	Approx. T ^b	Approx. Sig.
Nominal by Nominal	Lambda	Symmetric	,241	,212	1,036	,300
		Платформата за електронна търговия, която използвате е: Dependent	,083	,329	,243	,808
		Парола от клавиатура Dependent	,353	,164	1,809	,070
	Goodman and Kruskal tau	Платформата за електронна търговия, която използвате е: Dependent	,155	,119		,020 ^c
		Парола от клавиатура Dependent	,155	,117		,020 ^c
	Uncertainty Coefficient	Symmetric	,120	,095	1,258	,017 ^d
		Платформата за електронна търговия, която използвате е: Dependent	,125	,099	1,258	,017 ^d
		Парола от клавиатура Dependent	,115	,092	1,258	,017 ^d

Стойността на коефициента ламбда 0.353 показва, че връзката е сравнително силно интензивна.

При проверката на много от хипотезите също така не бяха открити връзки. Такъв пример е тестът между променливите *стойност на активите по балансова стойност и приоритет на информационната сигурност*, където стойността на χ^2 теста е 0,244933701635877, над критичното ниво и показва, че между променливите не съществува връзка.

Въпреки това можем да отбележим, че приоритетът на информационната сигурност е до вътрешна нагласа, преценка и мнение, а не толкова до финансови възможности. Независимо от финансовите възможности на организациите, за тях приоритетът на информационната сигурност може да е много висок.

Таблица 3.20

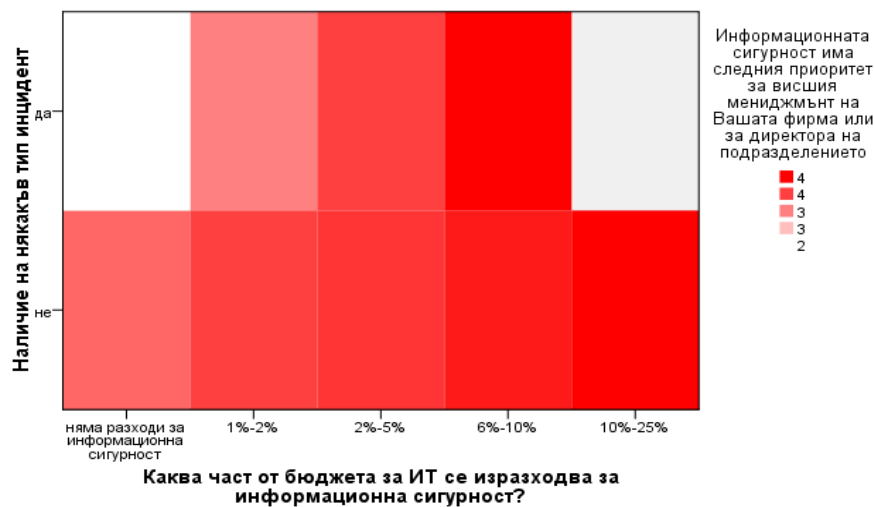
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	7,908 ^a	6	,245
Likelihood Ratio	6,714	6	,348
Linear-by-Linear Association	,421	1	,517
N of Valid Cases	33		

a. 10 cells (83,3%) have expected count less than 5. The minimum expected count is ,06.

Съществен момент при анализа с кростаблици е интерпретирането на информацията, дадена като забележка под таблиците с буквата **a**. Тази информация е относно нарушаването на една от предпоставките за χ^2 теста относно минимално очакваната честота за всяка клетка, която трябва да е 5 или повече. В определени случаи от направения анализ, коментарите под таблицата показват очаквана стойност под 5 за определени клетки, което показва отклонение от минималната честота за всяка клетка. В тези случаи съществува вероятност за опровергаване на направените изводи за наличие на статистически значима връзка между двете изследвани променливи. Единствено в таблица 3.18, където се търси връзка между променливите *разположение на платформата за електронна търговия* и *пароли от клавиатура като тип контрол на периметъра за достъп до данните*, не се извежда информация за клетки с очаквана стойност под 5. По този начин се потвърждава направения извод за наличие на статистически значима връзка между изследваните променливи.

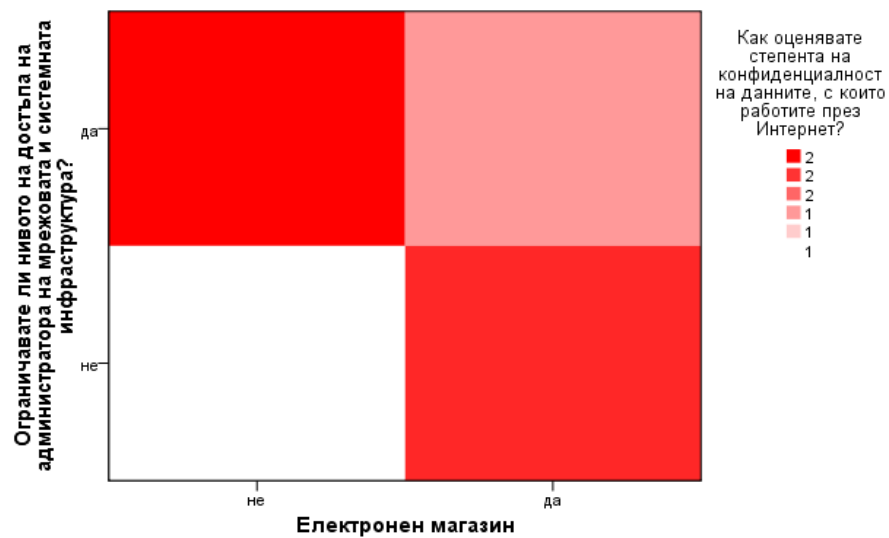
Графичните възможности на аналитичния софтуер SPSS на IBM позволяват по-атрактивно да представим връзките между променливите с така наречените „топлинни карти“.

Такава карта е илюстрирана на фиг. 3.21, която показва, че инцидент не е настъпил за организациите, за които приоритетът на информационната сигурност е най-висок, и частта от бюджета, изразходвана за информационна сигурност е между 15% и 20%.



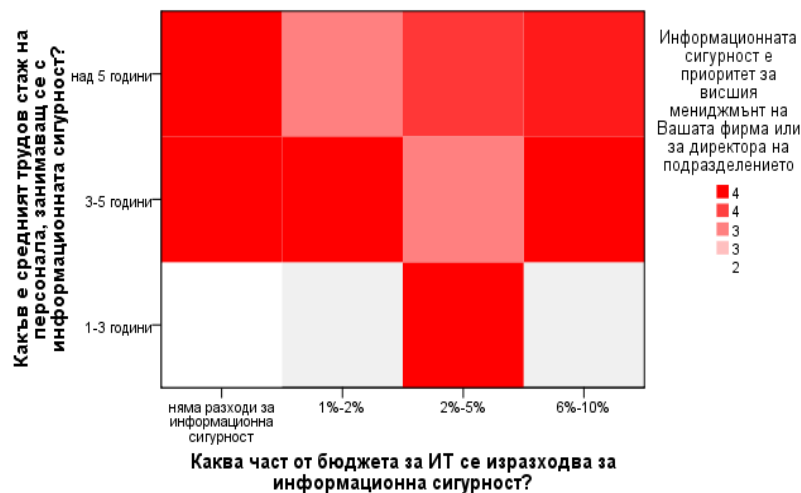
Фиг. 3.21. Код 4-много висок приоритет, код 3-висок приоритет, код 2- нисък приоритет

Следващата фигура 3.22 обвързва променливата *степен на конфиденциалност на данните, електронен магазин като избран модел за ЕТ и ограничаване нивото на достъп на администратора на инфраструктурата като техника за повишаване на информационната сигурност* и показва, че организациите, които не използват модела електронен магазин и ограничават нивото на достъпа определят степента на конфиденциалност на данните като най-висока.



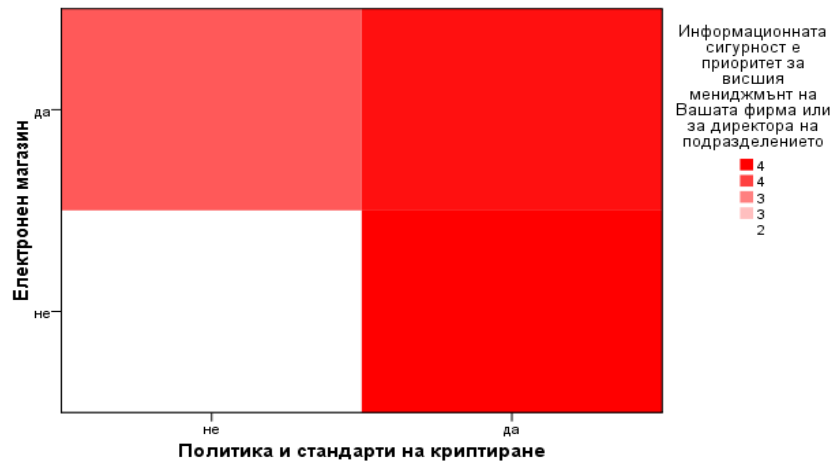
Фиг. 3.22. Код 2-конфиденциални, код 1-не са конфиденциални

Връзката между променливата *приоритет на информационната сигурност, среден трудов стаж на персонала, занимаващ се с информационна сигурност* и част от бюджета, изразходвана за информационна сигурност е илюстрирана на фигура 3.23. Тя показва, че приоритетът на ИС е най-висок за организации, при които персоналят, занимаващ се с ИС е със стаж между 3 и 5 години, като не е задължително разходите да са значителни.



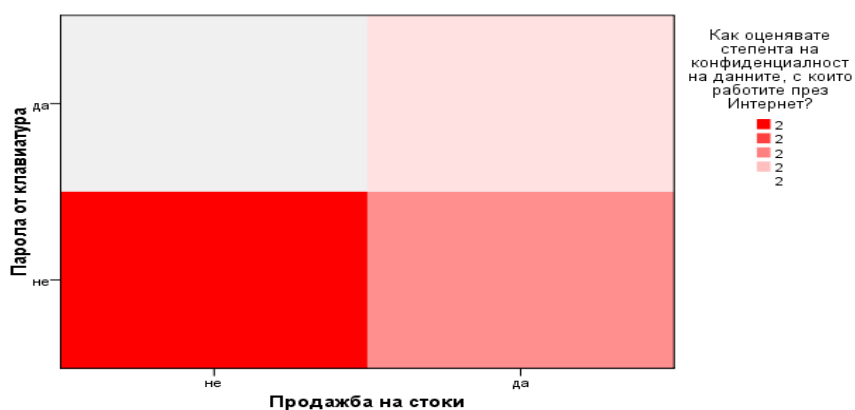
Фиг. 3.23. Връзка между приоритет на информационната сигурност, трудов стаж на персонала и разходи за информационна сигурност.

Следващата фигура 3.24 показва, че за организациите, където приоритетът на ИС е най-висок, политиката и стандартите на криптиране намират приложение и при модела електронен магазин, и при организации, които не са посочили електронен магазин като използван модел за ЕТ.



Фиг. 3.24. Връзка между електронен магазин политика и стандарти на криптиране и приоритет на информационната сигурност

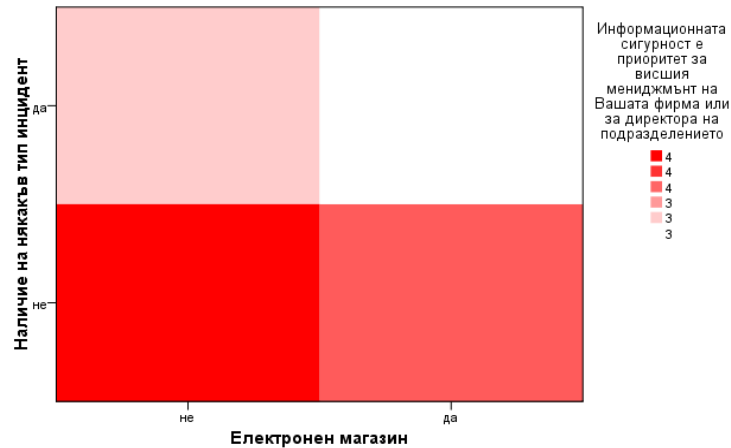
Следващата връзка включва променливите *степен на конфиденциалност на данните*, *продажба на стоки като област на извършване на ЕТ* и *парола от клавиатура като техника за контрол на периметъра за достъп до данните* и тя е илюстрирана на фиг. 3.25. Тук с най-висока степен на конфиденциалност са определени данните, собствениците на които извършват дейност в сфера, различна от продажба на стоки и не използват парола от клавиатура като способ за контрол на периметъра за достъп до данните.



Фиг. 3.25. Връзка между степен на конфиденциалност на данните, продажба на стоки и парола от клавиатура

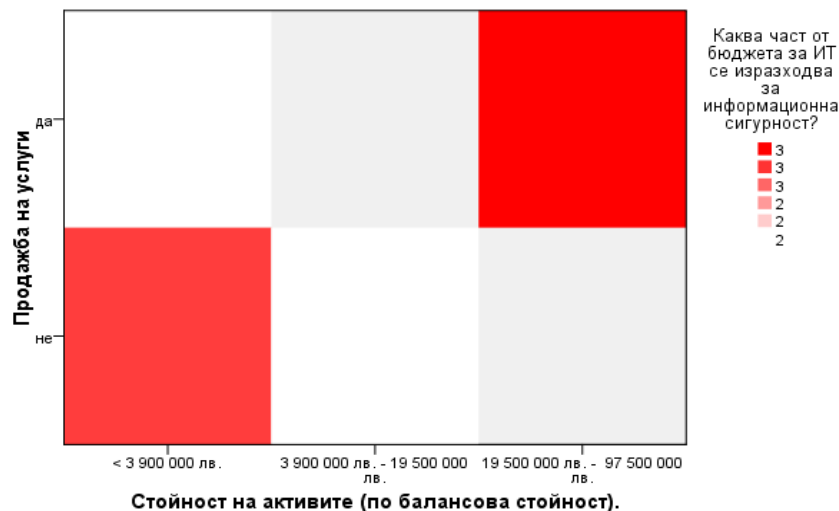
Една от може би най-важните връзки за изследването е връзката между най-използвания модел - *електронен магазин*, *приоритет на информационната сигурност* и *наличие на инциденти в сигурността*. Фигура 3.26 представя тази връзка и показва, че

организациите, използващи електронен магазин като модел за ЕТ и имащи най-висок приоритет на информационната сигурност, не са претърпели инцидент в сигурността за последната година.



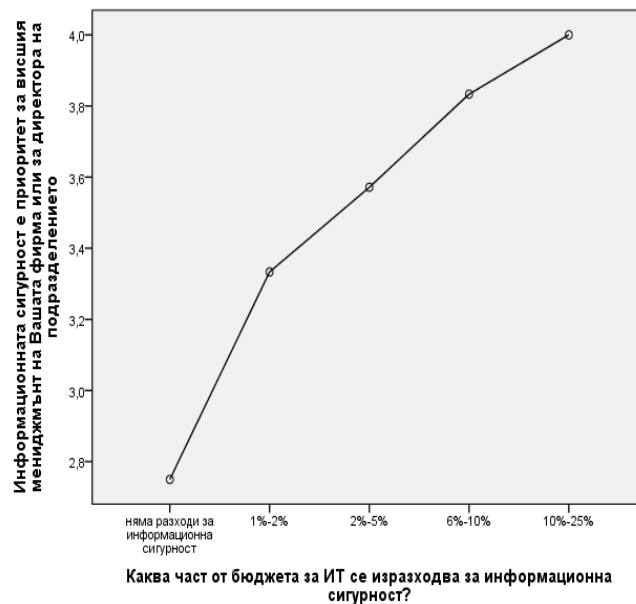
Фиг. 3.26. Връзка между приоритет на информационната сигурност, електронен магазин и наличие на инцидент в сигурността

Последната изследвана връзка обхваща променливите *стойност на активите, част от бюджета, използвана за информационна сигурност и продажба на услуги като област, в която се извършва ЕТ* и е показана на фигура 3.27. При нея разходите за информационна сигурност са най-високи за организациите, чиито активи са на стойност между 19 500 000 лв. и 97 500 000 лв. и извършват ЕТ в областта продажба на стоки.



Фиг. 3.27. Код 3-между 2 и 5%, код 2-между 1 и 2%

Зависимостта между променливите *приоритет на информационната сигурност и част от бюджета, изразходвана за информационна сигурност* е представена графично на фиг. 3.28.



Фиг. 3.28. Връзка между приоритет на информационната сигурност и част от бюджета, изразходвана за информационна сигурност

Зависимостта е правопрпорционална – с нарастването на приоритета на информационна сигурност, се увеличават и разходите.

3.2.3. Изводи от анкетното проучване

От направеното анкетно проучване на състоянието на информационната сигурност в системите за ЕТ на българските бизнес организации можем да направим следните изводи:

- Основната част от бизнес организациите, извършващи ЕТ спадат към групата на микро предприятията според ЗМСП, което предполага ограничени финансови средства за информационна сигурност.
- Именно поради ограничените финансови възможности, две трети от анкетираниите организации използват платформа, разположена на външен сървър, осигурен от доставчик на ИТ услуги. В този случай информационната система на електронния магазин се реализира и поддържа от доставчика на ИТ услугата.
- Съгласно нашето изследване, организациите, занимаващи се с ЕТ, са насочени предимно към продажба на стоки, а продажбата на услуги е направление, което би получило развитие в бъдеще;
- Почти всички респонденти определят много висок приоритет на информационната сигурност, въпреки че разходите, които са направили в това направление, са незначителни спрямо средните стойности на тези разходи в световен мащаб;
- Основните направления, в които се влагат средства за информационна сигурност, са: повишаване на ефективността, придържане към законите и наредбите и защита на репутацията на организацията;
- При една значителна част от респондентите не са регистрирани инциденти в сигурността, факт, който съществено се разминава със световните тенденции. Ситуацията в България можем да обясним с вида на бизнеса, които се определя като малък, липсата на данни, относно нарушения в сигурността, нежелание за споделяне на информация за пробиви и др.

При изследването бяха открити следните зависимости:

- бизнес организациите, за които приоритетът на информационната сигурност е най-висок, изразходват значителни средства - между 15% и 20% от бюджета си за информационна сигурност, инцидент при тях не е настъпвал;
- организациите, които не използват модела електронен магазин и ограничават нивото на достъпа, определят степента на конфиденциалност на данните като най-висока;
- приоритетът на информационната сигурност е най-висок за организациите, при които персоналът, занимаващ се с информационна сигурност е със стаж между три и пет години, като не е задължително направените разходи за информационна сигурност да са значителни;
- политиката и стандартите за криптиране намират приложение при организациите, в които приоритетът на информационната сигурност е най-висок, независимо дали се използва електронен магазин или друг модел за ЕТ;
- степента на конфиденциалност на данните се определя като най-висока при организациите, които извършват дейност в сфера, различна от продажба на стоки и които не използват парола, въведена от клавиатура като способ за контрол на периметъра за достъп до данните;
- организациите, които използват електронен магазин като модел за ЕТ и за тях приоритетът на информационната сигурност е най-висок, не са претърпели инцидент в сигурността за последната година;
- разходите за информационна сигурност са най-високи за организациите, чиито активи са на стойност между 19 500 000 лв. и 97 500 000 лв. и извършват ЕТ в областта на продажбата на стоки;
- съществува правопрпорционална зависимост между *приоритет на информационната сигурност* и *част от бюджета, изразходвана за информационна сигурност*.

3.3. Практически мерки за създаване на рамка за информационна сигурност в системите за електронна търговия

По настояще проблемите със сигурността на информацията при извършване на електронни транзакции и бизнес сделки са актуални, не само за България, а също и за най-развитите страни в света. За решаване на тези проблеми е необходимо първо да се изследва текущото състояние на информационната сигурност в организациите и на тази база да се предложат и реализират адекватни мерки и механизми, съответстващи на техните потребности и възможности.

3.3.1. Формиране на подход към създаване на политика за информационна сигурност

Разработването на политика за сигурност в ЕТ е наложителен и важен процес, който в значителна степен способства за нормалното функциониране и развитие на ЕТ.

Една от основните задачи на настоящия труд е дефиниране и изграждане на модел на политика за сигурност.

Моделът, който предлагаме, е съобразен и разработен за нуждите на организациите, които поддържат собствена инфраструктура за ЕТ, т.е. организации, които са разположили платформата за ЕТ на собствен сървър, поддържат от собствен ИТ персонал.

При организациите (малки и микро), които предоставят инфраструктура за ЕТ на трети страни и ползват платформа за ЕТ, собственост и хоствана от външен доставчик

на услуги, той осигурява основните аспекти на информационна сигурност на решението за ЕТ.

Бизнес организациите, използващи и поддържащи платформа за ЕТ на собствен сървър, трябва да отчитат спецификата на процесите вътре в организацията и на външната среда.

Отчитайки ситуацията в изследваните български организации, създаването на политика за сигурност се превръща в предизвикателство, което е повлияно от специфични особености, основните от които са:

- ограничените ресурси по отношение на финанси, специалисти и инфраструктура;
- подценяване на опасностите за сигурността на информацията;
- постоянно развитие на интернет технологиите;
- аутсорсингът почти не се използва;
- ограничени решения на СЕТ, които се използват от българските бизнес организации;
- трудности при създаването и спазването на вътрешни правила и процедури за сигурност;
- липса на подготвен персонал
- липса на допълнително обучение.

На база посочените особености на българските организации, може да се направи изводът, че компаниите, участвали в проучването ни и са активно присъстващи в Интернет, основно се стремят към разработването и функционирането на своя сайт, а проблемите със сигурността за тях остават на заден план. По този начин, още от началото на функциониране на организацията се пропускат основни изисквания за ефективна ЕТ, което в последствие ще доведе до негативни последици.

Подценяването на проблемите със сигурността на информацията от страна на изследваните организации се дължи на редица фактори (Върбанов Р. П., 2011). На първо място е **малкият бюджет за ИКТ**. Ограничените финансови възможности не позволяват на организациите да се сдобиват със съвременни технологии за защита и мрежово оборудване, поддръжката, на които ще изисква и влягането на допълнителни средства. На второ място е **подценяването и омаловажаването на ролята на технологиите за сигурност на данните и липса на ясна перспектива и стратегия**. При това положение СЕТ ще могат да реагират само на спешните случаи. По този начин се губят средства и усилията са насочени към възстановяване на нормалното им състояние, а не към разширяване на тяхната функционалност. На последно място трябва да отбележим, че **обучението и квалификацията на персонала** са от изключително значение за поддържането на високо ниво на информационна сигурност. В немалко случаи липсата на компетенции относно ключови принципи и процедури на сигурността са главната причина за реализирани пробиви, а не толкова зловредни програми или външни атаки.

За успешно и ефективно извършване на дейност в уеб пространството, е необходимо от самото начало при разработване на стратегията и оформяне на вижданията за търговия през Интернет, да се очертаят контурите на системата за информационна сигурност, която е и съществена част от глобалната система за сигурност в организацията. Този подход гарантира едновременно, че се вземат предвид организационните и технологичните проблеми, така и тези на информационната сигурност.

Създаването на политика за сигурност е първата стъпка при формирането на информационна сигурност. В този процес трябва да се вземат под внимание няколко ключови момента:

- изясняване на типа на данните и нивото, на което ще се защитават;
- уточняване на потенциалните нарушители и определяне на евентуалните щети, които могат да бъдат нанесени;
- анализи и идентифициране на рисковете и предприемане на мерки за тяхното редуциране;
- избор на конкретни технологии, методи и средства за осигуряване сигурност за ЕТ;
- тестване, имплементиране и поддръжка.

Изследването на специализираната литература (Върбанов Р. , Корпоративни мрежови архитектури и технологии, 2008) ни позволява да систематизираме 7 основни принципа, които да поставим в основата на подхода за разработване на политика за сигурност в ЕТ:

- автентификация – внедряване на подходящи механизми за идентифициране на потребителите и правата им за достъп, в съответствие с избрания модел за ЕТ и разработената стратегия за развитие;
- съхраняване на данните – принцип, свързан с необходимостта от избор на подходящо място за съхраняване на основната част от информацията за функционирането на СЕТ и решаване на проблема с достъпа до нея;
- обработване на поръчките – този принцип изисква включване на дейности, свързани с представяне на информация за поръчки, плащания с кредитни и дебитни карти и др.;
- постепенност и етапност – същността на този принцип изисква в началото да се избере нескъпа и сравнително стабилна и надеждна архитектура за система за защита, която да осигури определено ниво на сигурност на данните в организацията. В последствие при разширяване на функционалността, имплементираните решения да могат да се развиват и надграждат;
- въвеждане на водещи технологии и доказани решения в разглежданата област – според този принцип е препоръчително в началото на проекта за осъществяване на ЕТ да се планира използването на най-модерните решения за сигурност на данните и да се предвиди възможност за актуализация;
- защита на инвестициите – принцип, който изисква съхраняване на направените инвестиции чрез интегриране на наличното оборудване с новите технологии при насочване към по-комплексни и сигурни системи за сигурност;
- защита на транзакциите – според този принцип сървърът и клиентът трябва да бъдат защитени в процеса на комуникиране. Тук се включват възможности за използване на цифрови сертификати (Амор Д. , 2000).

Можем да обобщим, че проблемите със защитата и безопасността на информацията в българските бизнес организации, често са пренебрегвани и това влияе върху цялостното им функциониране. Формирането на подход за разработване на система от правила за защита на фирмените данни още в началния етап на изграждане на бизнес стратегията на организацията би способствало за сигурното и стабилно протичане на процесите в нея и би осигурило продължителното ѝ присъствие на пазара.

3.3.2. Елементи на рамката за информационна сигурност в системите за електронна търговия

В специализираната литература информационната сигурност на организацията се представя като сложен комплекс от нива, които формират една цялостна рамка на сигурността. За изграждане на рамката за информационна сигурност в СЕТ се базираме на

комплекса от йерархични нива, предложен от Янцевски (Janczewski, 2000). Авторът предлага осем нива за изграждане на информационна сигурност в организацията при извършване на ЕТ. Като използваме предложената от Янцевски рамка и вземем под внимание специфичните изисквания на СЕТ, считаме, че рамката за информационна сигурност на СЕТ трябва да включва:

Стратегия за сигурността, която се формира и се отнася за организацията като цяло, а не за отделни нейни подразделения, което означава, че е възможно стратегия за сигурността на ЕТ да не се разработва отделно, а тя да бъде част от глобалната стратегия за информационна сигурност. Тъй като ЕТ включва множество операции по предаване на чувствителна и секретна информация, считаме за целесъобразно да бъде разработена стратегия, която да бъде насочена точно към тези процеси и тяхната защита.

Политиката за сигурност, която се разработва като средство за постигане целите на стратегията за информационна сигурност и представлява съвкупност от процедури и правила, които трябва да се спазват от служителите в отделните звена. За разлика от стратегията, в политиката за сигурност трябва да се включат специфичните изисквания, които има СЕТ. Нейното проектиране преминава през различни фази, които ще бъдат разгледани подробно в т. 3.3.3.

Съгласуване на сигурността, което има отношение към процесите по развиване, обновяване или преустановяване на използването на различни приложения, свързани с ЕТ, и които изискват и прилагането на нови техники за информационна сигурност. Тяхното имплементиране трябва да се извърши много внимателно, като се следи да не се допуснат пропуски и уязвимости в сигурността.

Одитът, който е нужен за откриване на слабости и неточности в приложените мерки за сигурност и по този начин да се предотвратят бъдещи загуби. Съществен момент тук е формирането на правилен подход към идентифициране на недостатъци (ако има такива), конкретно за СЕТ и даването на препоръки за отстраняването им. Особено важно за сигурното функциониране на СЕТ е одитът да обхваща чувствителните области - достъп до системата, предаване на данни за банкови сметки и др.

Информираност относно сигурността на информацията, която се постига посредством програми за осведомяване, които започват с индивидуални разговори с всеки служител от момента на назначаването му. Тези програми е необходимо да се допълват с различни курсове през определен период от време за подобряване и мониторинг на информираността на персонала.

Обучение по въпросите на сигурността - имплементирането на стратегията и политиката за сигурност налага планиране на обучение по въпросите на сигурността във всички операции в СЕТ. То може да се извърши в различни форми, като класове, семинари и демонстрации. Това обучение не само може да повиши квалификацията на служителите, но също така и да допринесе за приемствеността на отговорностите по отношение на информационната сигурност.

Можем да обобщим, че информационната сигурност се изгражда като комплекс от отделни елементи, които са взаимосвързани. Всеки един от тези елементи има специфично предназначение и съдържа в себе си процедури и практики, които са насочени към повишаване на информационната сигурност. Правилното формиране на рамката за информационна сигурност и съставните ѝ елементи е отправна точка за реализирането на организационните процедури и технологиите, които ще се използват.

3.3.3. Методология за създаване на политика за сигурност

Успешното проектиране и създаване на политика за информационна сигурност на СЕТ, трябва да се извърши с участието на ключови кадри, към които спадат управители, финансови мениджъри, технически персонал, предоставящ информация за информационните ресурси. Също така е необходимо участие на персонал, който познава юридическите последствия от различните варианти на политиката.

За да бъде успешен този проект, трябва да се вземат под внимание няколко важни изисквания на СЕТ (Каео, 2006):

- Политиката за информационна сигурност да бъде изградена в хармония с българските и европейските стандарти и нормативни изисквания, най-важните от които са ISO 27001, ISO 27002, Законът за електронната търговия, Законът за електронният документ и електронният подпис и др.
- Политиката за сигурност да бъде в съответствие с глобалните за организацията принципи за информационна сигурност.
- Предварително дефиниране на ключовите, критично важни ресурси в СЕТ.
- Дефиниране инструментите за сигурност. Те могат да бъдат на физическо и на логическо ниво. Към физическото ниво се отнасят тези инструменти, които имат отношение към физическата инфраструктура, физическата сигурност на устройствата и физическия достъп. Те трябва да намерят приложение в началото на плана на корпоративната мрежа. Инструментите от логическото ниво създават граници между сегментите на мрежата и контролират потока на трафика между различните физически сегменти.
- Осигуряване цялост на системите и на данните. Тук се позиционира проблемът, изискващ трафикът в мрежата да бъде валиден и очакван, което означава да включва поддържани услуги, неподправени пакети и само данни, които не са били променени.
- Разработване на политики и процедури за персонала. Това изискване подвежда под отговорност всеки член от персонала относно поддръжката и обновяването на мрежовата инфраструктура, както и изискване служителите да разполагат със специално ръководство, според което да изпълняват своите задачи в съответствие с политиката за сигурност.
- Планиране обучение на персонала, което да включва адекватна подготовка относно многобройните проблеми и предизвикателства по отношение на сигурността. Обучението трябва да обхваща целия персонал, който проектира, имплементира или поддържа корпоративната мрежа и трябва да включва: техники по сигурност, методология и оценка на заплахи и слабости, критерии за избор и имплементация на инструменти, важноста на изложените на риск ресурси, за които не се прилагат механизми за сигурност.
- Извършване на внедряване на разработената вече политика за сигурност.
- Изпълнение на политиката, което да бъде проверявано и следено през определен период за откриване на слабости и проблеми в нея.
- Премахване на откритите проблеми, пропуски и слаби страни и актуализиране на политиката за сигурност.

В политиката за сигурност на СЕТ се изискват специални правила и процедури, когато се извършват трансакции с платежни карти. Изследователи от университета в Чикаго (ITservices, n.d.) считат, че правилата и процедурите, които трябва да се включат в политиката за сигурност и имат отношение към трансакциите с платежни карти, трябва

да бъдат съобразени с изискванията на стандарта PCI DSS⁵. Според този стандарт, персоналът, имащ достъп до информационните ресурси и съответно предаване и обработване на клиентските данни, трябва да бъде разделен в определени звена, всяко от които е с различни задължения и отговорности. Конкретните подразделения, които описват изследователите от чикагският университет, съгласно стандарта PCI DSS, включват: отдел информационна сигурност, системни администратори и проектанти, оперативен център за работа с данни, отдел мрежови услуги, отдел за поддръжка на работните станции, отдел корпоративни системи и приложение, отдел администриране на уеб системи и отдел притежатели на данни.

В предлаганата политика за информационна сигурност на СЕТ, няма да разглеждаме подробно тези правила и изисквания, тъй като в модела който развиваме, за електронните разплащания с дебитни и кредитни карти ще се използва доверена трета страна. За политиката на СЕТ, която планираме, сигурната връзка със системите за разплащане, които ще използваме, е изключително важна и с нея не могат да се правят никакви компромиси.

При проектирането и имплементирането на политика за информационна сигурност в СЕТ, Стоилов предлага да бъде следван йерархичен модел (Стоилов, Уязвимост на системите при свързване на корпоративните мрежи с мрежите за управление на технологични процеси, 2010). Авторът формулира структура на модел на политика за сигурност, комбинирайки политическите декларации от високо ниво, стандартите и процедурите, както и ръководствата за конфигуриране. Към този модел предлагаме да бъде добавено и ниво *одит на информационната сигурност* (вж. фиг.3.29).



Фиг. 3.29. *Нива на политиката за сигурност, източник: (Стоилов, Уязвимост на системите при свързване на корпоративните мрежи с мрежите за управление на технологични процеси, 2010)*

Фигура 3.29 представя примерен модел на политика за сигурност, отделните нива, които го съставят, тяхната подчиненост и субординация.

Според Стоилов, процесът на създаване на политиката за сигурност може да бъде разделен на девет отделни стъпки:

- **осигуряване на подкрепа от ръководството** - тази стъпка е задължително да бъде извършвана до пълното установяване на параметрите на сигурността в мрежата;

⁵ Стандарта е описан подробно в Глава II т.2.3.

- **определяне на информационните ресурси** – извършва се чрез подробна инвентаризация на всички хардуерни и софтуерни ресурси и провеждане на разговори на всички нива на управленската структура;

- **проект за политическа декларация** - политиката за сигурност трябва да е лесна за четене и потребителят трябва лесно да се ориентира в нея. Самият документ трябва да се състои от следните части: **въведение (резюме), контекст, декларация за политика, дефиниции, органи / отговорности, промени в политиката за сигурност, достъпност на информацията;**

- **оценка на риска** - изграждането на политиката за сигурност е многоетапен процес - първо се определя какво трябва да се защити, след това се определя от кого трябва да се защитават данните и вероятните рискове;

- **избор на мерки за противодействие** - противодействието може да бъде техническо решение, но то също така може да бъде и административно или физическо решение;

- **създаване на стандарти за сигурност** - документи, които описват какви технологии, административни процедури и физически контрол ще бъдат приложени, за да се подкрепи избраната политика за сигурност;

- **създаване на ръководства за конфигуриране** - целта на документацията за конфигуриране е тя да служи като ръководство на органите за управление на информационната сигурност;

- **прилагане на политиката за сигурност** - политиката за информационна сигурност се разпространява до всички служители в организацията във форма, достъпна и разбираема за тях. Прилагането на политиката за сигурност се изразява в спазване на предварително дефинирани процедури, които показват как да се защитят информационните ресурси;

- **преразглеждане и изменение на политиката за сигурност** - политиката за информационна сигурност се преразглежда периодично на базата на установен процес или след основни промени в защитата на информацията и в нея да се внасят необходимите изменения и допълнения.

Към **одита на информационната сигурност** в СЕТ предлагаме да се включат процедури по проверка на стриктното спазване на установените дейности по отношение на сигурността, както и откриване на различни несъответствия или неефективно действащи контролни дейности.

Отчитайки принципите и спецификата на състоянието на информационната сигурност в организации от малък и среден тип, които се явяват преобладаващата част организации, които са участвали в нашето проучване, Върбанов предлага методология за разработване на политика за сигурност, която включва 8 отделни фази (Върбанов Р. П., 2011). Тези фази са (вж. фиг.3.30):

- уточняване на целите и задачите на информационната сигурност в организацията;

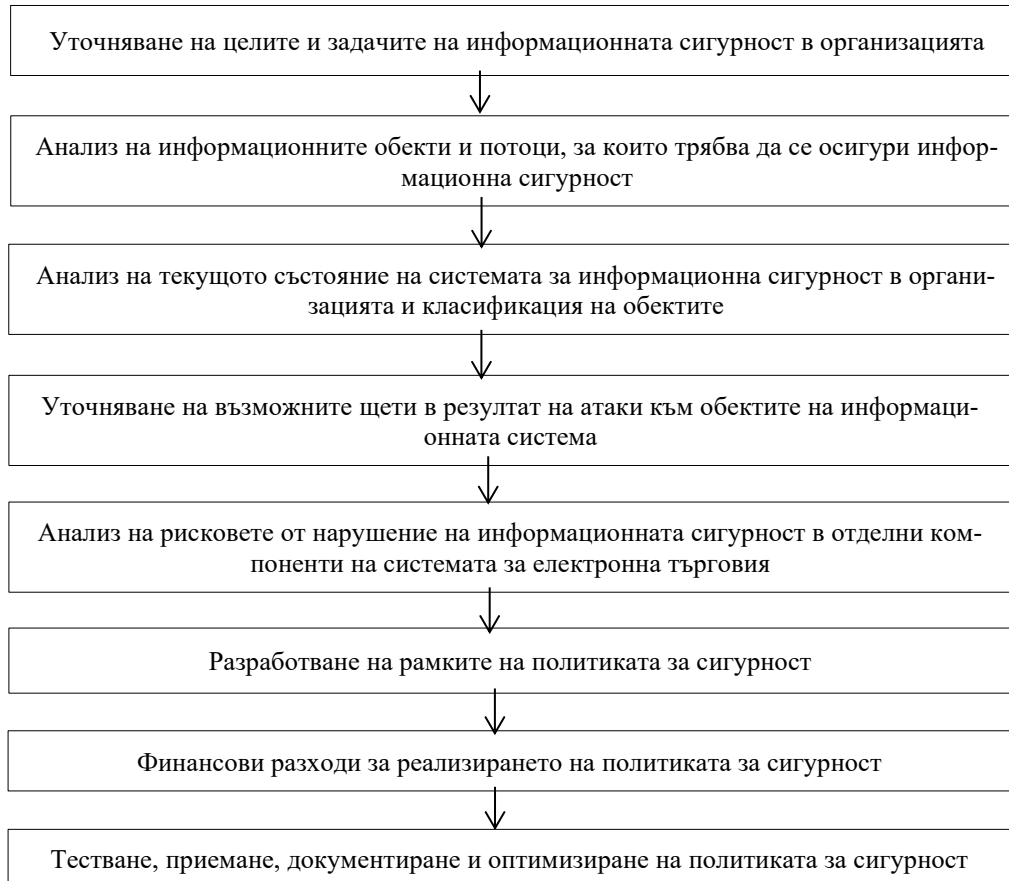
- анализ на информационните обекти и потоци, за които трябва да се осигури информационна сигурност;

- анализ на текущото състояние на системата за информационна сигурност в организацията и класификация на обектите;

- уточняване на възможните щети в резултат на атаки към обектите на информационната система;

- анализ на рисковете от нарушение на информационната сигурност в отделни компоненти на СЕТ;

- разработване на рамките на политиката за сигурност;
- определяне на финансовите разходи за реализирането на политиката за сигурност;
- тестване, приемане, документиране и оптимизиране на политиката за сигурност.



Фиг. 3.30 *Методология за създаване на политика за сигурност на ЕТ в малки и средни предприятия, източник: (Върбанов Р. П., 2011)*

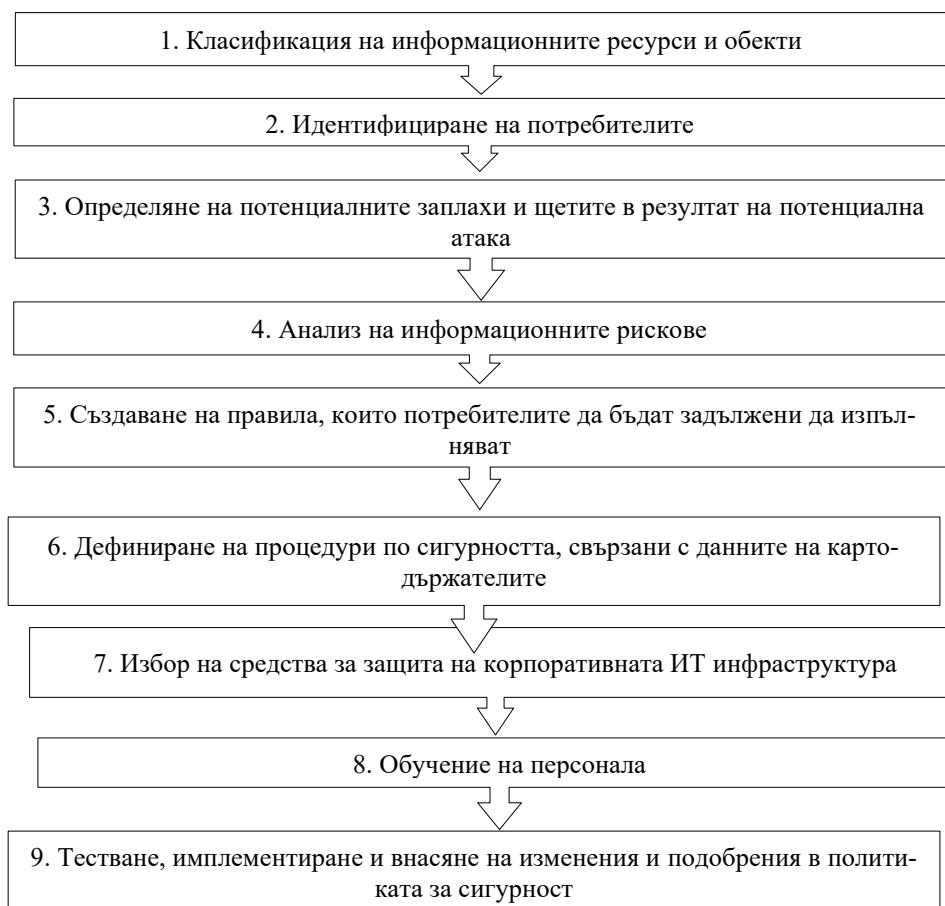
Коментиранията методология можем да разширим, като добавим още и: система от правила, касаещи съхраняването и обработването на данните на притежателите на банкови карти за разплащане; обучение на персонала.

Формулираната от цитираните автори, политика за сигурност преследва следните цели:

- осигуряване на непрекъснатост на процесите в организацията и фокусиране върху разрастването на бизнеса, а не върху възстановяване след проблеми;
- минимизиране на рисковете за сигурността на информацията, причиняващи загуби или вреди;
- идентифициране на основните параметри на политиката за информационна сигурност;
- минимизиране на степента на загуби или вреди, резултат от пробиви в сигурността.

Постигането на изброените цели изисква решаването на четири основни задачи - осигуряване на достъпност, конфиденциалност, цялостност и отговорност на информацията.

Изследвайки опита на различните автори и множеството научни публикации в тази област, считаме, че в съдържателно отношение методологията за разработване на политика за сигурност, която да е приложима в българските бизнес организации, осъществяващи ЕТ, трябва да включва няколко основни стъпки (вж. фиг. 3.31):



Фиг. 3.31 Методология за разработване на политика за сигурност

Стъпка 1: Идентификация и класификация на всички информационни ресурси и обекти, които имат отношение към ЕТ и изискват определени нива на защита. Тези ресурси и обекти включват:

- уеб сървърът;
- уеб сайтът или електронния магазин;
- използваната мрежа, която може да бъде публична или частна;
- служителите на организацията;
- клиентските данни, съхранявани в организацията и др.

Стъпка 2: Идентифициране на всички потребители, ползващи различни информационни ресурси. Необходимо е да се разграничат правата на различните нива потребители – вътрешни потребители, клиенти, информационни посредници, партньори и др.

Стъпка 3: Определяне на потенциалните заплахи и уточняване на щетите за организацията в резултат на атака. Тук е необходимо да се анализират всички точки на достъп и евентуален пробив в системите и да се приложат различни математически методи за изчисляване на определени показатели и стойности, които да служат като отправна точка за предприемането на противодействащи мерки при съответна стойност.

Стъпка 4: Анализ на информационните рискове. Тук намират приложение подходите за анализ на риска – количествен и качествен и съответстващите им методи и показатели – годишна честота на реализация, очакване за единична загуба, очаквана годишна загуба и др. Въз основа на коректно извършения анализ на риска могат да се използват различни техники за прехвърляне, смекчаване, поемане или избягване на риска.

Стъпка 5: Създаване на правила, които потребителите да бъдат задължени да изпълняват. Тези правила зависят от статуса на потребителя и включват дейности, които трябва да се следват при работа със системните ресурси и да гарантират индивидуалната отговорност на всеки служител към принципите на информационната сигурност в организацията.

Стъпка 6: Дефиниране на процедури при обработването на данните на притежателите на банковите карти за разплащане. Тези процедури включват избягване съхраняването на чувствителни данни за картите, предаване на данните съгласно определени правила за сигурност и премахването им след приключване на транзакцията или след определен период от време.

Стъпка 7: Избор на средства за защита на корпоративната ИТ инфраструктура, като трябва да се отчита, че колкото по-мощни и сложни стават корпоративните системи, толкова повече защитата на отделен участък от тях става недостатъчна. Тук трябва да се вземе предвид, че развиването на корпоративната ИТ инфраструктура налага имплементиране на съответни комплексни техники за сигурност, които са насочени към новата функционалност и в същото време не са в конфликт с вече внедрените.

Стъпка 8: Обучение на персонала по въпросите за сигурността, разработените правила и процедури и очакваните ефекти от внедряването на политиката за сигурност. Това обучение има за цел формиране на информационна култура в служителите и създаване на навици за сигурно извършване на операциите със системните ресурси.

Стъпка 9: Тестване, имплементиране и внасяне на изменения и подобрения в политиката за сигурност.

Разработването на политика за сигурност, базирана на изложената методология отчита спецификата на българските бизнес организации и формира рамка за дефиниране на съответно поведение, определяне базата за необходимите средства, избор на подходящи контроли и създаване на необходимите процедури. Формално разработената политика за сигурност трябва да включва няколко ключови раздела, препоръчани от Британският стандарт BS 7799 (Daniel, 2003):

- **въведение**, което потвърждава намеренията на висшето ръководство за реализиране политика на информационна сигурност;
- **организационен**, който съдържа описание на подразделенията, комисиите, групите и т.н., отговарящи за информационната сигурност на организацията;
- **класификационен**, който описва съществуващите в организацията материални и информационни ресурси и необходимите нива на сигурност;

- **щатен**, който характеризира мерките за сигурност, прилагани към персонала: *описание на длъжностите от гледна точка на информационната сигурност, организация на обучение, порядък за реагиране на нарушенията на сигурността на информацията* и т.н.

- **физическа защита** - раздел, който описва подходите и средствата за физическа защита;

- **управление на компютри и мрежи** – раздел, който описва използваните подходи за управление;

- **правила за разграничаване на достъпа** – отнасящ се до фирмената информация;

- **разработка и съпровождане на системите** - раздел, който характеризира порядъка и процесите за разработка и съпровождане;

- **непрекъснатата работа** - раздел, който описва мерките, насочени към осигуряване на непрекъснатата работа на организацията;

- **юридически раздел**, който потвърждава съответствието на политиката за сигурност с действащото законодателство.

Резултатната политика за сигурност трябва да бъде съхранявана на хартиен носител и да притежава следните ключови характеристики (Каео, 2006):

- политиката да може да се имплементира технически;
- политиката да може да се имплементира организационно;
- политиката да може да се налага посредством инструменти за сигурност и наказания в зависимост от ситуацията;

- политиката ясно да дефинира сферите на отговорност на потребителите, администраторите и ръководството;

- политиката трябва да бъде гъвкава и да може да се адаптира към променящата се среда.

Смятаме, че за да се гарантира и поддържа високо ниво на сигурност на информацията в СЕТ е много важно да се следват и прилагат някои добри и доказали се практики, като тези, предложени от Шиф (Schiff, 2013):

- **избиране на сигурна платформа за ЕТ** – поставянето на сайта за ЕТ на платформа, която използва сложни обектно-ориентирани езици предполага по-голяма сигурност от използването на такава с отворен код;

- **използване на защитена връзка за онлайн поръчка** – използването на защитена Security Socket Layer (SSL) връзка за уеб удостоверяване и защита на данните ще даде сигурност на клиентите, че сайта е безопасен и са предприети сериозни мерки за защита на информацията, която те трябва да предоставят;

- **да не се съхраняват чувствителни данни** – да се избягва съхраняване на хиляди записи на клиенти, особено на данните за кредитни карти. Препоръчително е старите записи от базата данни да се премахват периодично и да се поддържа минимално количество данни, достатъчно за връщане на средствата на клиентите и за възстановявания;

- **включване на система за проверка на валидността на кредитни карти** – използването на такава система допринася за предпазване от плащане на измамни такси, свързани с използването на картата;

- **изискване на трудни за разгадаване пароли** – към клиентите могат да се поставят изисквания за минимален брой символи и цифри, което е от тяхна полза за осигуряване на по-високо ниво на безопасност;

- конфигуриране на система за сигнали при подозрителни действия - задаване на предупредителното известие за множество и съмнителни сделки, извършени от един и същ IP адрес, или сигнали за множество поръчки, направени от едно и също лице с различни кредитни карти, телефонни номера, които са от подчертано различни райони в сравнение с адреса за фактуриране и системи, където името на получателя е различно от името на притежателя;
- наслояване на сигурността – това е един от най-добрите начини за поддържане на бизнеса в безопасност от киберпрестъпници. Добавянето на допълнителни слоеве за сигурността на сайта и приложения като контактни форми, логин форми и заявки за търсене ще гарантира, че ЕТ се опазва от околната среда от прилагането на атаки;
- осигуряване на обучение относно информационна сигурност за работниците и служителите - служителите трябва да бъдат образовани по отношение на законите и политиките, които засягат данните на клиента и да бъдат обучени на необходимите действия, за да ги държи в безопасност;
- използване на проследяващи номера за всички поръчки – използват се за предотвратяване на измами при плащания;
- редовен мониторинг на сайта – наблюдението на взаимодействията на потребителите със сайта в реално време позволява да се открие подозрително поведение при извършването на транзакциите;
- редовни сканирания на системата – извършването на такива сканирания намалява риска, че платформата за ЕТ е уязвима за хакерски атаки;
- редовно архивиране - съществува риск от загуба на ценна информация в случай на прекъсване на хранването, недостатъчен капацитет на твърди дискове, вирусни атаки. При настъпване на някое от изброените, трябва да се гарантира, че сайтът ще функционира безпроблемно.

Можем да заключим, че предложената методология за създаване на политика за информационна сигурност в СЕТ обобщава съществуващия опит в областта на безопасността на ЕТ и предлага решение, подходящо за българските организации от тази сфера. Ние считаме, че разработването и практическата реализация на методологията за безопасност на СЕТ е целесъобразно да се възложи на външна организация. По редица причини по-малките организации не са в състояние да решават задоволително целия комплекс от проблеми, свързани с безопасността на бизнеса в Интернет.

Трябва да отбележим и факта, че в България аутсорсингът на информационни технологии добива сериозна популярност за малките организации и с разрастване на инициативите за ЕТ и все по-мащабното навлизане на ИКТ в тази сфера, може да се очаква тенденция към повишено търсене на ИТ услуги на външни компании.

3.3.4. Архитектурен модел на решение за информационна сигурност в системите за електронна търговия

Едно от направленията на рамката за информационна сигурност в СЕТ е архитектурен модел на решение за информационна сигурност, който да представи в по-детайлен вид основните компоненти и връзките между тях. В предложения модел следваме принципите и изискванията, поставени с политиката за сигурност.

След извършено проучване на специализираните литературни източници, посветени на различни аспекти на сигурността – сайт за ЕТ, електронните разплащания, мобилни устройства и др., в които изследователи и специалисти от практиката предлагат свои модели, можем да направим следното систематизиране:

Софтуерният архитект Даршананд Кусиал от компанията IBM изследва текущото състояние на приложенията за ЕТ и представя модел, който се основава на веригата на стойността и гарантира сигурността при онлайн пазаруването (Khusial, n.d.).

В трудовете си изследователите Ваххария, Мишра и Кумар от своя страна представят общ модел на ЕТ, където основните отношения са бизнес към бизнес (B2B), бизнес към клиент (B2C), клиент към бизнес (C2B) и клиент към клиент (C2C) (Vakharia, 2013). Основните точки на уязвимост в този модел се свеждат до клиент, клиентски компютър, мрежова връзка между клиент и търговец, сървър на търговеца и доставчик на софтуерни услуги. За сигурност на клиента могат да се приложат електронни сертификати, защитни стени за филтриране на трафика, антивирусен софтуер и механизмите на криптиране. При отношенията бизнес към бизнес могат да намерят приложение защитени канали за комуникация, виртуални частни мрежи, протоколите SSL и TLS, както и протоколите за удостоверяване (Kerberos, Radius и др.) и задължителна актуализация на сървърните и клиентските операционни системи. За защита на електронните разплащания задължително препоръчваме използване на стандартите PCI DSS и 3-D Secure и протоколите SSL и SET.

Други изследователи като Юсуф Каркахия поставят обучението в основата на модела на сигурност (Qarkaxhija). Това обучение, ще насочи купувачите към инсталиране на персонални защитни стени, използване на механизми за криптиране, криптиране на информационните потоци между клиента и уеб сайта чрез протокола SSL, прилагане на адекватни политики по отношение на паролите, защитните стени и рутинни външни одити, както и анализ на заплахите, стриктни политики за развитие и вътрешни одити.

Експертите от компанията Rackspace предлагат стратегия за ЕТ, в която се акцентира на следните аспекти и особености (Rackspace):

- прилагане на системи, които са изцяло ориентирани към клиента;
- избор на платформа за ЕТ, като се има предвид и план за пренасочване към друга платформа;
- сайтът на електронния магазин да предлага функционалност за мобилни устройства;
- избор на мерки за сигурност и съответствие, продиктувани от бранша, в който е бизнеса на организацията;
- готовност за най-натоварения трафик, включително на тестване на натоварването и сравняване на резултатите.

Трябва да отбележим, че тези елементи от своя страна налагат внедряването на специфични организационни и технологични механизми за защита, които според нас могат да бъдат Bring Your Own Device (BYOD) политика по отношение на мобилните устройства, гарантиране на отказоустойчивост, прилагане на стандарта PCI DSS.

Специалистите-практици от PowerSource считат, че разработването на ефективна политика за сигурност на ЕТ изисква включване на планове за предоставяне на сигурна онлайн среда, заедно с по-задълбочени данни за съоръженията за архивиране на данните, целящи справяне с кризисни ситуации (Powersource, n.d.). Според тях, ефективният план за сигурност на ЕТ трябва да обхваща четири основни детерминанти - поверителност, автентификация, интегритет и потвърждаване. Безспорно осигуряването на тези елементи може да се реализира с методите на криптиране, цифрови подписи, протоколът SSL и инсталирането на защитни стени.

Изследователите от университета в Северна Каролина Антон и Ърп предлагат модел за защита на системите за ЕТ, който се състои от следните елементи: идентифициране на ресурси, центрирани около софтуер, хардуер, хора и документация; оценка и

приоритизиране на тези ресурси; идентифициране на рисковете и слабите места, включително и вероятностите за всеки от тях; определяне на политиката на приемлива употреба въз основа на работна етика и култура; определяне на необходимите предпазни мерки, включително физическа сигурност, одит и реагиране при инциденти; създаване на план за поетапно въвеждане на политика; информация за политиката за потребителите в рамките на организацията, както и подходящи външни лица като партньори (Anton).

Изпълнението на този план е свързано с прилагане на методите за анализ на риска, както и стандартите за информационна сигурност, които са насочени към разработване на системи за информационна сигурност, като ISO 27001 и ISO 27002.

В разработката на Найду откриваме много полезно организационно структуриране на процеса по създаване на методологията за защита (Naidu, n.d.). Авторът предлага следните етапи: проектиране на политиката за сигурност като съвкупност от политики; след проектирането, политиката трябва да се внедри и да започнат операциите по спазването ѝ; при спазването на политиката трябва да се извършва мониторинг, с цел елиминиране на неточности; откритите проблеми се отстраняват с актуализиране на политиката; политиката трябва да бъде функционална и точно спазвана.

При изграждането на тази политика могат да намерят приложение стандартите за информационна сигурност и технологии като защитни стени, антивирусен софтуер и др.

Специалистите от института SAN насочват вниманието си към подсигуриране на сайта за ЕТ, като за изграждането на информационната сигурност се взема предвид не единствено уеб сървър, а всички фактори (SANS, n.d.). Тук приложение намират защитните стени, протоколите за сигурност на информацията, защитните механизми в сървърните операционни системи и антивирусният софтуер.

Експертите от Екипа за реагиране на компютърни инциденти (Computer Security Incident Response Team CSIRT) Глеснер, Келерман и Макневин предлагат модел, като представят връзките между основните участници с електронните транзакции – клиент, платформа за ЕТ, финансови институции, хостинг компании и доставчици на софтуерни инструменти (Glaessner, 2002). За защита на тези връзки могат да се използват защитни стени, системи за откриване на нарушители, приложения за тестване за прониквания, антивирусен софтуер.

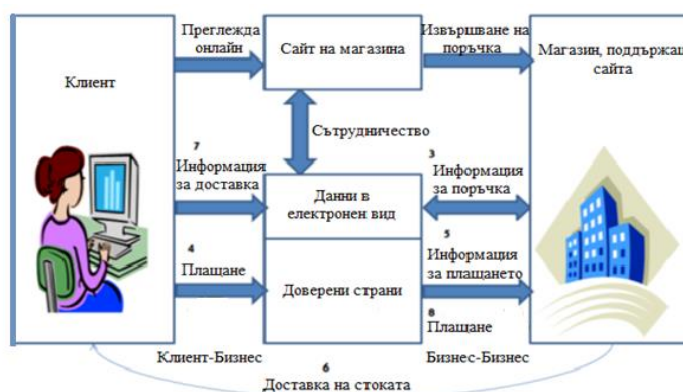
Според нас, разработването, въвеждането в действие и поддържането на ефективен модел за сигурност в ЕТ предполага следването на **три основни стъпки**:

- 1. Дефиниране на основните участници в онлайн сделките.**
- 2. Идентифициране на заплахите при комуникирането между тях.**
- 3. Предприемане на мерки срещу тези заплахи.**

За да идентифицираме **основните участници** в ЕТ използваме моделът на Вакхария и други автори, според който те са: клиент; сайт за ЕТ; магазин, поддържащ сайта; доверени страни (системи за електронни разплащания) (вж. фиг.3.32). Към тях можем да добавим и доставчици на софтуерни приложения за ЕТ, които също се явяват участници в процеса на осъществяване на ЕТ, още и злонамерени лица (хакери, кракери и др.).

В резултат на извършеното проучване на литературните източници, в които се предлага модел на СЕТ, считаме, че моделът, предложен от Вакхария, Мишра и Кумар най-пълно и точно отразява компонентите на решението за ЕТ, участниците, взаимодействието и връзките между тях. Този модел ще използваме като база, която ще разширим и детайлизираме.

Основните взаимодействия в този модел са: клиент към бизнес; бизнес към доставчик на приложения; отношения между страните на електронните транзакции; бизнес към бизнес. Тези взаимодействия дефинират типа на потенциалните заплахи и точки на уязвимост за СЕТ. Нашият модел е насочен към защита в тези точки.



Фиг. 3.32. Общ модел на ЕТ, източник: (Vakharia, 2013)

Отношения клиент към бизнес

Според нас основните заплахи в тях се свързват с измама и подвеждане на клиентите от страна на злонамерени лица, проникване в клиентския компютър, атаки към уеб сайта с цел получаване на неоторизиран достъп и подслушване на мрежовия трафик. Ключовите точки са три – клиент, сайт на електронния магазин, магазин, поддържащ сайта и връзките между тях.

Защитата на клиента е обект на множество анализи и проучвания. Защитената комуникация между клиента и сайта за ЕТ поставя големи предизвикателства пред информационната сигурност, защото клиентите са много на брой, с различни познания в областта на ИТ, използващи различни софтуерни и технологични платформи. За поддържане на високо ниво на сигурност в отношенията клиент към бизнес можем да препоръчаме използване на предложените от Кусиал и Маккинги техники (Khusial D. M., n.d.):

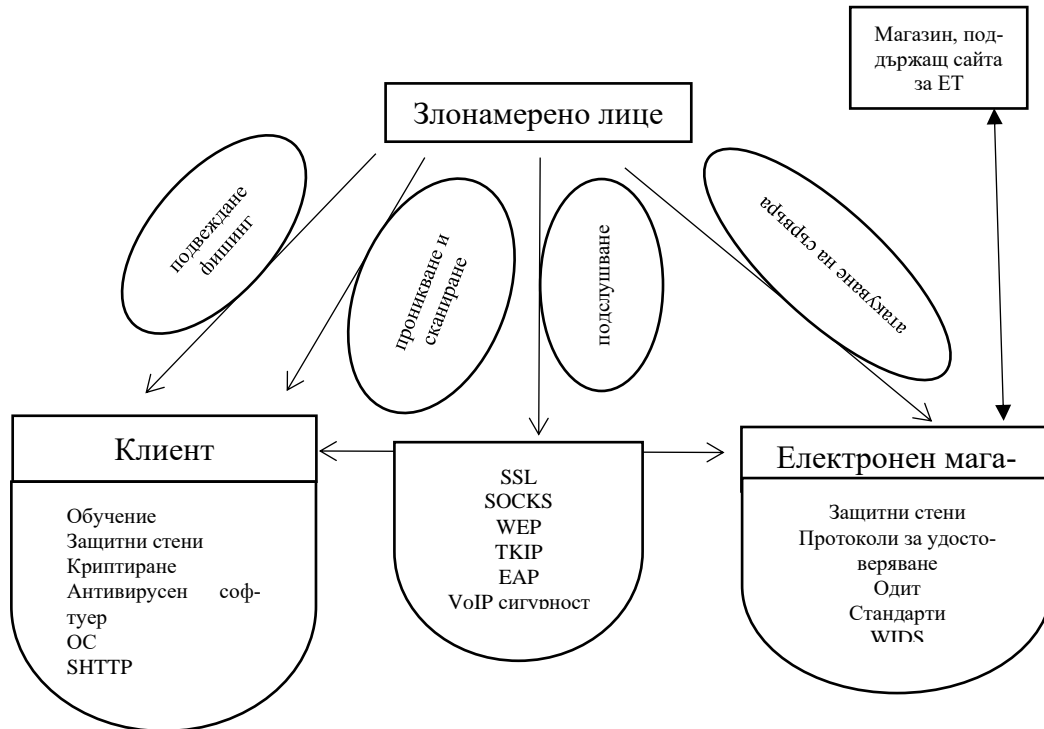
- обучение и придобиване на информационна култура по отношение на сигурността;
- инсталиране на защитни стени;
- криптиране на данните, съхранявани в потребителския компютър.

Към тези техники можем да допълним - използване на протокола SHTTP за комуникиране със защитени съобщения, протоколът S/MIME за защита на електронната поща, инсталиране на антивирусен и антишпионски софтуер, както и добавяне на последните актуализации към клиентските операционни системи.

По отношение на мрежовите връзки, считаме за задължително приложението на протокола SSL за криптиран трафик между комуникиращите страни. Той може да бъде допълнен от протокола SOCKS, за реализиране на мрежова защитна стена. В тази област може да се приложат и протоколите за: защитен мобилен достъп WEP, TKIP, EAP Transport Layer Security, EAP- Tunneled TLS, EAP- Tunneled TLS, Protected EAP, когато ще се използва безжична мрежа; протоколите за VoIP сигурност при комуникация с лоялни или преференциални клиенти.

Според нас сигурните взаимоотношения клиент към бизнес, включващи злонамерени лица и видовете заплахи, дейностите, които трябва да се извършат и технологиите, които трябва да се използват от страната на клиента и електронния магазин, протоколите, които трябва да гарантират сигурността на комуникациите са представени на фиг. 3.33.

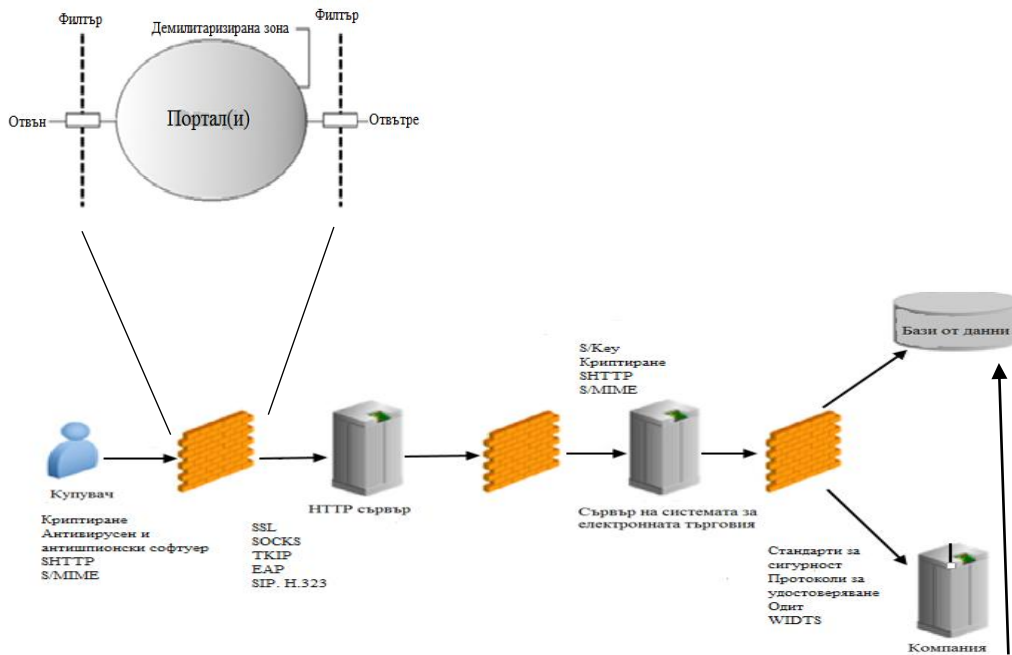
За сигурността на електронния магазин са приложими множество технологии и механизми. В тази връзка експертите от Oracle препоръчват задължително филтриране на трафика със защитна стена (Oracle). Към нея можем да допълним и сървър за удостоверяване като: TACACS+; RADIUS; Kerberos; FORTEZZA.



Фиг. 3.33. Заплахи и техники за защита на взаимодействието клиент към бизнес

От изключително значение е да бъдат разработени и прилагани политики, относно използването на пароли, които строго да се изпълняват, както от външните, така и от вътрешните потребители. Целесъобразна практика е да се извършват периодични одити на достъпа до вътрешните системи, както и актуализиране на сървърните операционни системи. Тъй като все повече потребители предпочитат да пазаруват през мобилните си устройства, считаме за строго препоръчително да бъдат прилагани системи за засичане на безжични прониквания – Wireless Intrusion detection Systems (WIDS). Не на последно място трябва да отбележим и необходимостта от сертифициране по водещите стандарти за информационна сигурност, като ISO 27001, ISO 27002, Common Criteria и др.

Обособените компоненти, осигуряващи взаимодействията клиент към бизнес с използваните технологии за информационна сигурност в тях, са представени на фиг. 3.34.

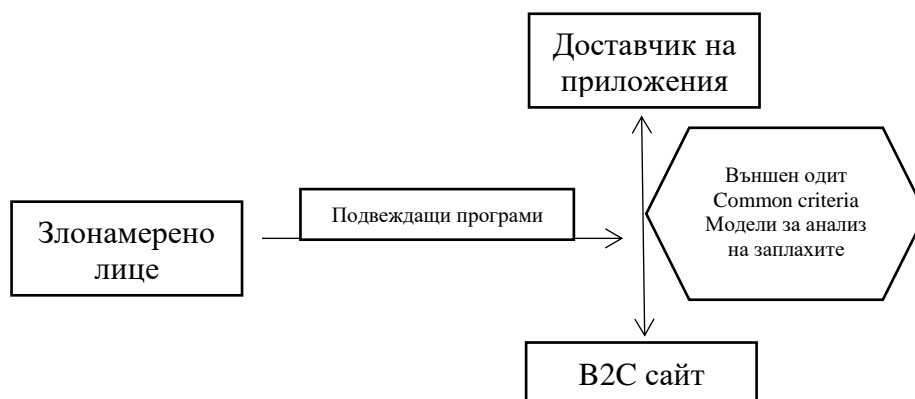


Фиг. 3.34. Защитена връзка между клиент и сайт на електронен магазин, източник: (Oracle)

Отношения бизнес към доставчик на приложения

Изследванията в това направление са насочени към защита на вътрешната корпоративна инфраструктура и предпазване от внедряването на зловредни и подвеждащи приложения. В тази насока специалистите от IBM препоръчват използването на външни одити и модели за анализ на заплахите, които да установят стриктното спазване на съответните техники и процеси, свързани с приложенията (Khusial D. R., н.д.).

Считаме, че съществено приложение тук също може да намери и стандарта „Общи критерии за информационна сигурност“ (Common Criteria), който дава насоки за развитието на специфични СЕТ, както и за развитието на софтуер, предоставян от външни организации и използван като инфраструктура за сайтове на електронни магазини.



Фиг. 3.35. Сигурност при отношенията бизнес към доставчици на приложения

Отношения между страните на електронната транзакция

Защитата на данните в процеса на заплащане е задължителна, поради факта, че трансферът на данни относно банкови карти, пароли за достъп до сметки и др. може лесно да бъде прихванат от злонамерени лица. В това направление експертите от Webmenshirts препоръчват стандартния протокол за създаване на криптирана връзка между клиент и сървър SSL, чрез които данните се криптират със 128-битов ключ (Webmenshirts, n.d.).

В допълнение на SSL можем да поставим протокола защита на електронните транзакции - Secure Electronic Transaction (SET), чрез които с помощта на електронни сертификати и криптирана връзка се гарантира сигурността на данните.

Сравнението на протоколите в таблица 3.21 показва по-широката функционалност на SET, което предполага насочване към него като основен протокол за защита на електронните транзакции.

Таблица 3.21

Сравнение между протоколите SSL и SET

Възможности	SSL	SET
Криптиране на данните по време на трансфера	Да	Да
Потвърждение за интегритета на съобщението	Да	Да
Автентификация на търговеца	Да	Да
Автентификация на клиента	Не	Да
Трансфер на специфични данни с определен базис	Не	Да
Включване на банка или доверена трета страна в сделката	Не	Да
Не е нужно търговецът вътрешно да подсигурява данните за банкови карти	Не	Да

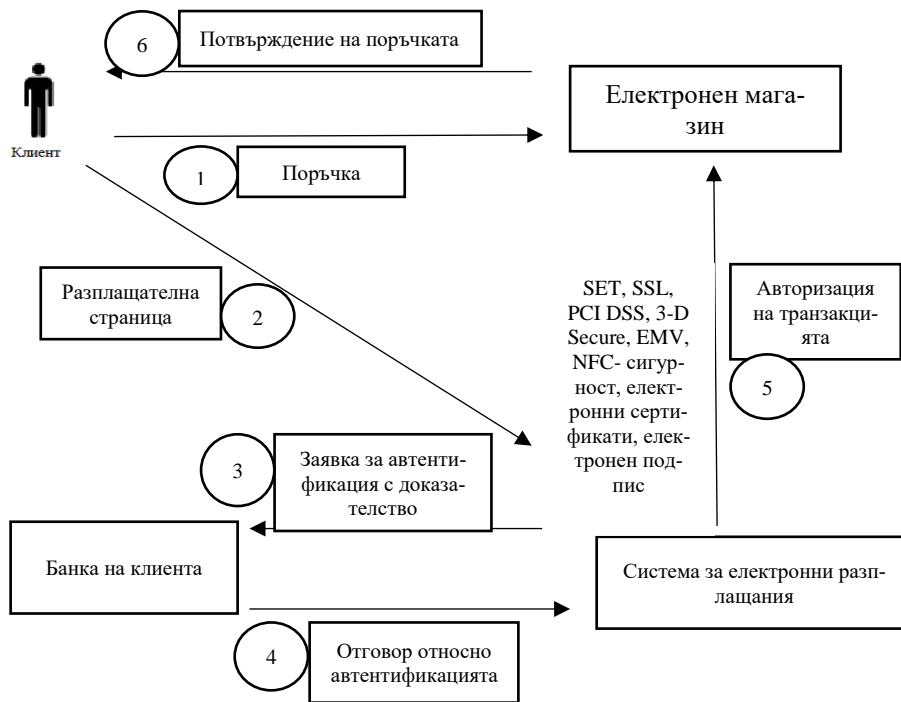
Източник: (Uky, n.d.)

Поради бързото разрастване на безконтактните плащания, е наложително да се обърне внимание и на сигурността на мобилните системи за заплащане, осъществявани чрез технологията Near Field Communications (NFC) и използване на платформи на мениджъри за сигурни услуги (Trusted Service Manager Platform).

Като ефективно средство, гарантиращо в най-голяма степен, че единствено физическият собственик на подписа с неговия персонален идентификационен код (ПИН) ще може да се идентифицира и да подписва онлайн плащания, в отношенията между платежните системи и страните на електронната транзакция може да се използва електронния подпис.

Допълнителни средства за повишаване на информационната сигурност в тази насока може да се включват стандартите за сигурност на електронните заплащания с карти: PCI DSS; 3-D Secure; EMV.

Компонентите и връзките между тях в SET, обработващи електронните транзакции са показани на фиг. 3.36.



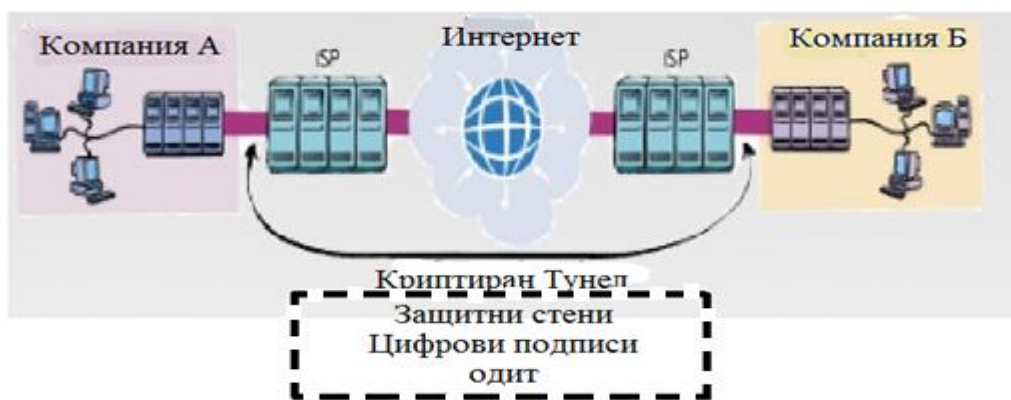
Фиг. 3.36. Сигурно плащане, източник: (Webmenshirts, н.д.)

Отношения бизнес към бизнес

Комуникациите между бизнес организации съдържат критична фирмена информация, чието попадане в неоторизирани и злонамерени лица може да доведе до катастрофални последици за компанията.

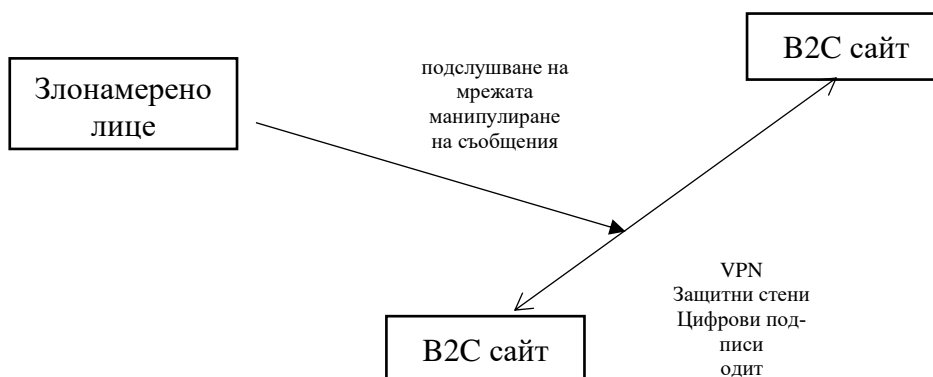
Сигурността на тези връзки е предизвикателство, над което са работили редица експерти. Сигурна защита на тези връзки е подсигурияването с виртуални частни мрежи (VPN) за тунелиране и криптиране на съобщения и изпращането им по защитени канали, според Реболо от университета във Валенсия (Rebollo, н.д.) и др.

Към използването на VPN можем да прибавим защитни стени за филтриране на трафика, одити на достъпа до вътрешната мрежа, цифрови подписи и сертификати, както и протоколите за сигурно комуникиране.



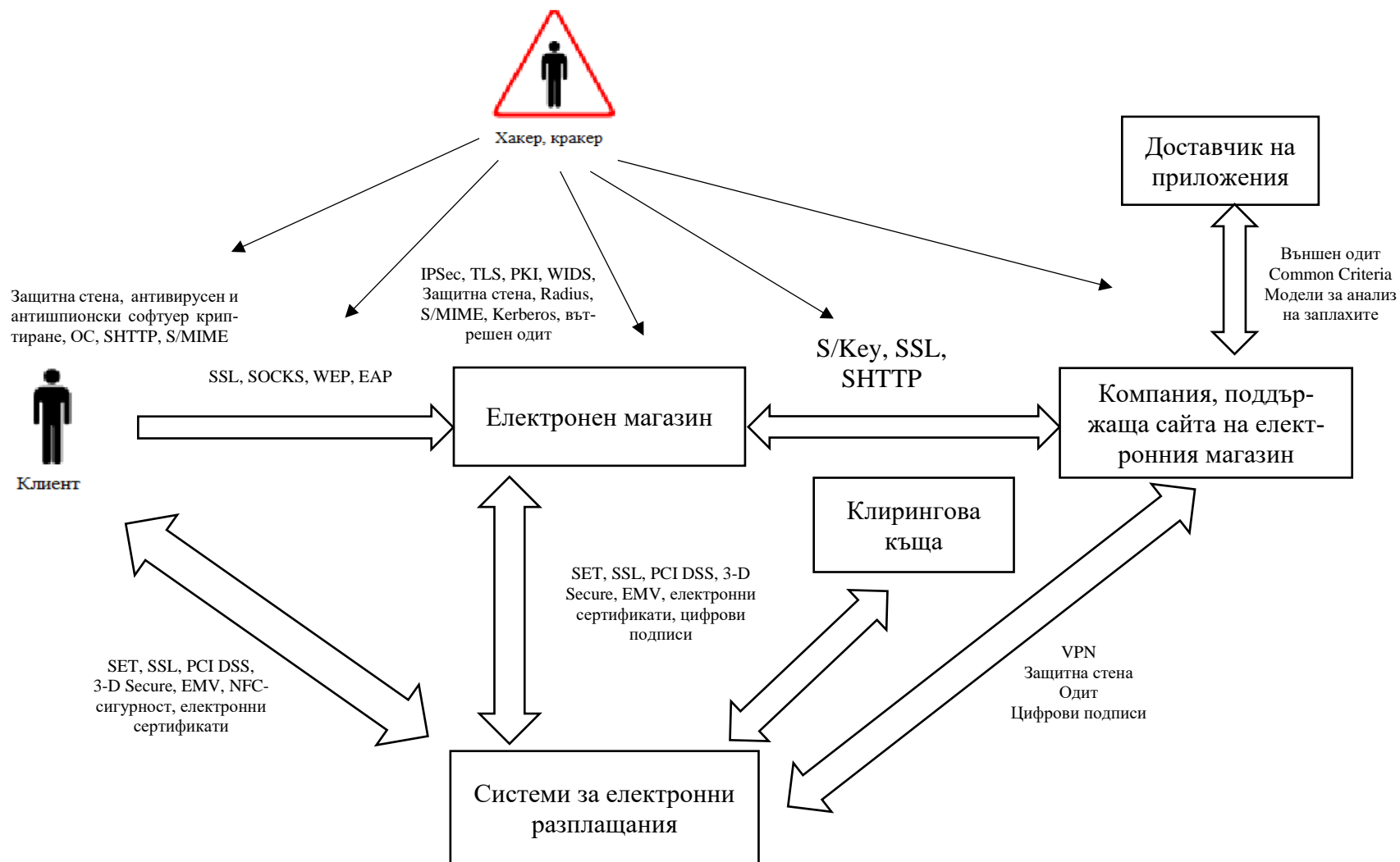
Фиг. 3.37. Виртуални частни мрежи и защита на комуникациите между две компании, източник: (Rebollo, н.д.)

Организацията на отношенията бизнес към бизнес са представени на фиг. 3.38.



Фиг. 3.38. Сигурност при B2B отношенията

След направения анализ на заплахите в отношенията между участниците в ЕТ и възможните средства и дейности за повишаване на сигурността, моделът на Вакхария, Мишра и Кумар (вж. фиг.3.32), който използвахме като отправна точка в решението за информационна сигурност в СЕТ, може да бъде детайлизиран и допълнен, както е показани на фигура 3.39.



Фиг. 3.39. Обобщен модел на информационната сигурност в SET

В обобщение можем да заключим, че предложеният модел е опит максимално задълбочено да се анализира спецификата на връзките и взаимодействията в СЕТ с цел да се предложат подходящи мерки и да се приложат цялостни практики за информационна сигурност. Следването му може в значителна степен да гарантира сигурното протичане на процесите в СЕТ, както и стабилността на организацията в Интернет пространството.

В резултат на изследването на състоянието, политиката и стратегията за информационна сигурност на ЕТ в български организации и предлаганите от нас решения, можем да формулираме следните **основни изводи**:

1. В условия на финансова криза, българските бизнес организации избягват сериозни инвестиции в която и да е област. Техните бюджети са ограничени и това води до недостатъчни средства, както за нови технологични решения, така и за квалифициран персонал за информационна сигурност. Най-популярните решения за ЕТ са използване на платформа, разположена на външен сървър, предоставен от доставчик на ИТ услуги. Основните проблеми в българските организации, развиващи ЕТ, са липсата на осведоменост и култура по отношение на информационната сигурност.

2. Приоритетът на информационната сигурност за почти всички български организации, участвали в нашето изследване, е много висок, въпреки че за повечето от тях направените разходи са незначителни, спрямо средните в световен мащаб. Основните направления, в които се правят разходи за информационна сигурност, са: повишаване на ефективността; придържане към законите и наредбите; защита на репутацията на организацията.

3. Липсата на инциденти в сигурността на българските организации (за разлика от световните тенденции) можем да обясним с това, че в сферата, която изследваме (ЕТ от тип В2С), участват главно малки организации (ограничени ресурси), не се публикуват данни за нарушенията в сигурността - организациите не желаят да споделят информация за пробиви в техните системи.

4. Проблемите със сигурността на информацията в българските бизнес организации често са пренебрегвани и това оказва влияние върху цялостното им функциониране. Формирането на подход за разработване на система от правила за защита на фирмените данни, още в началния етап на изграждане на цялостната бизнес стратегия на организацията, би способствало за сигурното и стабилно протичане на процесите в нея и ще повлияят върху продължителното ѝ присъствие на пазара.

5. Информационната сигурност се изгражда като комплекс от отделни елементи, които са взаимосвързани и формират една цялостна рамка на сигурността. Всеки от тези елементи има специфично предназначение и включва процедури и практики, насочени към повишаване на информационната сигурност. Правилното формиране на рамката за информационна сигурност и съставните ѝ елементи е отправна точка за реализирането на организационната и технологичната сигурност.

6. Методологията за създаване на политика за информационна сигурност в СЕТ, която представяме, обобщава съществуващия опит в областта на безопасността на ЕТ и предлага ефективно решение, което е съобразено с условията, в които функционират българските организации от тази сфера. Ние считаме, че разработването и практическата реализация на методологията за безопасност на СЕТ е целесъобразно да се възложи на външна организация. По редица причини по-малките организации не са в състояние да решават задоволително целия комплекс от проблеми, свързани с безопасността на бизнеса в Интернет.

7. Архитектурният модел, който предлагаме, отчита спецификата на връзките и взаимодействията в СЕТ. Целта му е да се предложат подходящи мерки и да се приложат

цялостни практики за информационна сигурност. Смятаме, че следването на предложени модел може в значителна степен да гарантира сигурното протичане на процесите в СЕТ, както и стабилността на организацията в Интернет пространството.

Заклучение

Информационната сигурност е основен и жизненоважен приоритет за ефективното функциониране на системата за електронна търговия. Тя има сложна и многоплатова природа. За да е резултатна, информационната сигурност трябва да съчетава адекватни на бизнес средата технологии, закони, политики, процедури и индустриални стандарти.

Изследването на информационната сигурност в системите за електронна търговия в българските организации дава представа за текущото състояние и е база за изследователско търсене на възможности за нейното усъвършенстване, дефиниране рамка за политика за сигурност, с прилагането на която ще се постигне желаното високо ниво. В тази връзка са решени няколко основни задачи, които включват: критичен анализ на състоянието на информационната сигурност в системите за електронна търговия от тип В2С в български организации; изясняването на подхода за създаване на политика за информационна сигурност и разширяване на рамката за информационна сигурност с нови елементи; разработване на методология за политика и изграждане на модел за информационна сигурност, който да е в съответствие със състоянието и потребностите на бизнес средата и технологичното обкръжение на български организации, осъществяващи ЕТ

Вследствие на извършеното проучване на теоретичните основи на информационната сигурност в електронната търговия и изследване на практиката на българските организации, съобразно стратегическите цели и задачи на разработката могат да се направят следните изводи:

А. В теоретичен аспект

За сега цялостният размер на киберпрестъпленията не може да бъде точно определен, в същото време киберпрестъпленията срещу сайтовете за ЕТ бързо нарастват, в резултат на което загубите на организациите се увеличават и управлението на сайтовете за ЕТ трябва да се подготви за противодействие на разнообразни криминални атаки.

Защитата в ЕТ има шест ключови измерения - *интегритет, неотричане, автентичност, конфиденциалност, секретност и наличност*.

Въпреки че компютърната защита се счита за необходима за предпазването на дейностите, свързани със СЕТ, тя не е без недостатъци. Съществуват две основни области на напрежение (противоречие) между защитата и оперирането в уеб сайта, които се отнасят до *лекотата на използване и обществената безопасност*.

Най-широко разпространените форми на заплаха за сигурността на сайтовете за ЕТ включват: *вредителски код; потенциално нежелана програма; фишинг; хакери и кибер вандализъм; измами с кредитни карти; спуфинг; отказ от обслужване и разпределена атака отказ от обслужване; подслушване; вътрешни атаки; лошо проектиран сървърен или клиентски софтуер; проблеми със сигурността на социалните мрежи; проблеми със сигурността на мобилните устройства; проблеми със сигурността на облачните изчисления и др.*

Едно от възможните решения на тези заплахи е криптирането на информацията, чрез което се осигуряват четири от шестте ключови измерения на сигурността на ЕТ - *интегритет на съобщението, неотричане, автентичност и конфиденциалност*.

Решенията, които може да използваме са криптиращи технологии включващи: *криптиране със семантичен ключ; криптиране с публичен ключ; криптиране с публичен ключ, използвайки цифров подпис и хеш функция; цифров плик; цифрови сертификати и инфраструктура с публичен ключ*.

В допълнение към криптирането, съществуват множество други инструменти, които се използват, за да защитят комуникационните канали в Интернет. Те включват *Secure Socket Layer (SSL)* и *виртуални частни мрежи (VPNs)*.

След подsigуряването на комуникационните канали, следва защитаване на мрежите, сървърите и клиентите, за което се използват и различни инструменти, като *защитни стени, прокси сървъри, контрол на операционните системи* и *антивирусен софтуер*.

Функционирането на организациите в Интернет пространството изисква задълбочени анализи и изследвания, с цел да бъдат минимизирани заплахите за сигурността. На тази база организациите, реализиращи ЕТ, трябва да развият последователна и ясна корпоративна политика, която се съобразява с природата на: всички явни и потенциални рискове; информационните ресурси, които трябва да бъдат защитавани; необходимите процедури и технологии, които да посрещнат рисковете; механизмите за прилагане и одитинг. Необходимо е също и разработване и приемане на обществени закони срещу киберпрестъпленията.

Съставянето на план за защита е ключов етап от функционирането на организациите, от формирането на уеб сайта и през целия период на съществуване на организацията. Процесът включва няколко основни стъпки - *извършване оценка на риска, разгръщане на политика за защита, създаване на план за изпълнение, създаване на екип по сигурността* и *осъществяване на периодични одити на защитата*.

Системите за онлайн разплащане играят съществена роля в СЕТ. Основните видове съвременни системи от този тип са *онлайн транзакции с кредитни карти, PayPal, алтернативни системи за плащане като Amazon Payments, Google Wallet и Bill Me Later*, българските системи *Epay.bg, Easypay, eBG*, *мобилни системи за плащане* и *цифрови пари*. Системите за електронно фактуриране и плащане (ЕВРР systems) са форма на система за онлайн плащане на месечни сметки/фактури. ЕВРР - услугата позволява на клиента да види електронните сметки и да ги плати чрез трансфериране на електронни фондове от банкови сметки или кредитни карти. Основни участници на ЕВРР пазара са *системи за директно плащане на сметки, консолидатори* и *доставчици на инфраструктура*, които поддържат моделите директни сметки и консолидатор.

Б. В практико-приложен аспект

В резултат на изследването на състоянието, политиката и стратегията за информационна сигурност на ЕТ в български организации и предлаганите от нас решения можем да формулираме следните основни изводи;

- В условия на финансова криза българските бизнес организации избягват сериозни инвестиции за нови технологични решения и защита. Преобладаващата част от изследваните компании, осъществяващи ЕТ, са микро и малки предприятия, които нямат собствена ИТ инфраструктура и собствен ИТ персонал.

- Информационната сигурност е от голямо значение за преобладаващата част от организациите, извършващи ЕТ, въпреки това в политиката и стратегията за информационна сигурност на организациите не се отделя необходимото внимание на политиката за управление на данните.

- Разходите за информационна сигурност, правени от българските бизнес организации, са значително по-малки, съпоставени със средните в света. Безпокойство поражда фактът, че 23% от изследваните организации не правят разходи за информационна сигурност, а други 17% правят много малки разходи – 1% от бюджета за ИТ.

- Методологията за създаване на политика за информационна сигурност в СЕТ предлага ефективно решение, което е съобразено с условията, в които функционират

българските организации от тази сфера. Ние считаме, че разработването и практическата реализация на методологията за безопасност на СЕТ е целесъобразно да се възложи на външна организация. По редица причини по-малките организации да не са в състояние да решават задоволително целия комплекс от проблеми, свързани с безопасността на бизнеса в Интернет.

- Архитектурният модел, който предлагаме, отчита спецификата на връзките и взаимодействията в СЕТ. Целта му е да се предложат подходящи мерки и да се приложат цялостни практики за информационна сигурност. Смятаме, че следването на предложения модел може в значителна степен да гарантира сигурното протичане на процесите в СЕТ, както и стабилността на организацията в Интернет пространството.

Основните приноси и резултатите от настоящия труд са в следните насоки:

1. Изяснена е същността на понятието информационна сигурност и други, свързани с него понятия, а също така е извършен анализ на защитата като основен компонент на СЕТ.
2. Направен е критичен анализ на съвременните информационни и комуникационни технологии, подходи, решения и стандарти, поддържащи защитена среда за функциониране на електронната търговия от тип В2С.
3. Извършен е критичен анализ на база организирането и провеждането на анкета с участието на специалисти от практиката за установяване на текущото състояние на информационната сигурност в СЕТ от тип В2С на бизнес организации в България.
4. Изяснен е подходът за създаване на политика за информационна сигурност и е разширена рамката за информационна сигурност с добавяне на нови елементи.
5. Разработена е методология за политика и е изграден модел за информационна сигурност, който е в съответствие със състоянието и потребностите на бизнес средата и технологичното обкръжение на български организации, осъществяващи ЕТ.

Използвана литература

1. Амор, Д. (2000). *Еволюцията на Е-бизнеса*. София: ИнфоДар.
2. Амор, Д. (2000). *Еволюцията на Е-бизнеса*. София: ИнфоДар.
3. Биткойн. (2013). *Биткойн България*. Retrieved 02 05, 2015, from <http://www.bitcoin.bg/>: <http://www.bitcoin.bg/>
4. Бойчев, Б., Шишманов, К., & Маринова, К. (2016). Състояние и перспективи в използването на банкови карти като средство за разплащане (разплащателен инструмент) в България. *Алманах научни изследвания*, 23, 35-64.
5. Буюклиева, С. (2007). *Криптографски хеш функции*. ВТУ.
6. Върбанов, Р. (2004). *Основи на електронния бизнес*. Велико Търново: Абагар.
7. Върбанов, Р. (2008). *Корпоративни мрежови архитектури и технологии*. Академично издателство „Ценов“.
8. Върбанов, Р. (2009). Безопасността на електронната търговия: Рискове и възможни последици. *Народностопански архив*.
9. Върбанов, Р. П. (2011). Изследване на състоянието и сигурността на данните в бизнес ин-формационните системи на малки и средни предприятия и разработване на политика и стратегия за информационна сигурност. *Алманах Научни изследвания*.
10. Георгиев, А. (2014). *Интернет търговията в България продължава да расте*. Retrieved 12 5, 2014, from www.regal.bg.
11. Глазков, А. А. (n.d.). *Опыт автоматизации разработки профилей защиты и заданий по безопасности по ISO/IEC 15408*. Retrieved 05 29, 2013, from <http://www.bezpeka.com/>: <http://www.bezpeka.com/ru/lib/spec/metr/art182.html>
12. Горшков, В. С. (2003). *Электронная коммерция и национальная безопасность. Защита информации*.
13. Груев, Г. (n.d.). *Пет водещи тенденции в електронната търговия*. Retrieved 06 24, 2013, from <http://www.regal.bg/>: <http://www.regal.bg/show.php?storyid=1945723>
14. Димитров, З. (2010). *Защита на фирмените онлайн комуникации*. *ew business* .
15. Дюкенджиев, Г. (2008). *Инструменти за анализ и управление на качеството*. София: СУ.
16. Емилова, П. (2002). *Усъвършенстване на дейността на фирмите посредством електронен бизнес*. Свищов: АИ „Ценов“.
17. Емилова, П. М. (2006). *Информационни технологии*. Свищов: АИ „Ценов“.
18. Илиев, Й. (2012). *Анализ на риска за информационната сигурност: системи и заплахи*. *СИО*.
19. *Информационна сигурност*. (n.d.). Retrieved 03 15, 2014, from <http://profisec.bg/>: <http://profisec.bg/bg/700/informatsionna-sigurnost>
20. *Ипотпал противодействие и ипотпал защита*. (n.d.). Retrieved 04 13, 2013, from <http://ipotpalweb.wordpress.com/>: http://ipotpalweb.wordpress.com
21. Каео, М. (2006). *Проектиране на мрежова сигурност*. Софтпрес.
22. Краева, В. К. (2009). *Електронен бизнес*. Велико Търново. Фабер.
23. Кръстева, Н. (2011). *ИТ сигурността в българските организации - в дисонанс с глобалните тенденции*. *СИО*.
24. Кръстева, Н. (2011). *Кибер престъпниците залагат капани в социалните мрежи*. *СИО*.
25. Кръстева, Н. (2013). *Вътрешните заплахи за ИТ сигурността – масово явление*. *СИО*.
26. Кръстевич, Т. С. (2010). *SAS и SPSS за начинаещи: Подготовка, визуализация и анализ на данни*. Свищов.

27. НСИ. (n.d.). *Национален осигурителен институт*. Retrieved 08 15, 2014, from <http://www.nssi.bg/>: <http://www.nssi.bg/eservicesbg/reports/42-pik>
28. Орсов, З. (2001). *СЮ. Практически аспекти на закона за електронния документ и електронния подпис*.
29. CSB. (n.d.). *СИСТЕМА ЗА УПРАВЛЕНИЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ*. Retrieved 04 20, 2013, from <http://www.csb-hold.com>: <http://www.csb-hold.com/iso27001.php>
30. Семерджиев, Ц. (2007). *изурност и защита на информацията*. София: Класика и Стил.
31. *Сигурност и защита на информацията в Интернет - Идентификация на потребителя*. (n.d.). Retrieved 03 27, 2013, from <http://www.antivirus.trbk.net>: <http://www.antivirus.trbk.net>
32. Станев, С. (n.d.). *Компютърни мрежи и комуникации*. Retrieved 04 29, 2013, from <http://bg.convdocs.org>: <http://bg.convdocs.org/docs/index-1530.html?page=28>
33. Стоилов, Е. (2010). Уязвимост на системите при свързване на корпоративните мрежи с мрежите за управление на технологични процеси. *Автоматика и информатика*.
34. Стоилов, Е. (2011). *Управление на мрежовата сигурност*. София.
35. Стоилов, Е. (2011). *Управление на мрежовата сигурност. Системи за откриване на нарушители*. София.
36. Шишманов, К. (2004). *Електронна търговия и електронни разплащания*. Велико Търново: Абагар.
37. Шишманов, К. К. (2007). *Информационни системи и експертни оценки в застрахователното дружество*. В. Търново: Абагар.
38. Эймор, Д. (2001). *Электронный бизнес – эволюция и/или революция*. Вильямс.
39. Янкова, Д. (n.d.). *Пазаруване от колективни сайтове*. Retrieved 10 10, 2013, from www.novinar.bg: www.novinar.bg
40. *A Guide to Securing Red Hat Enterprise Linux*. (2013). Red hat.
41. Alibaba. (n.d.). *Alibaba.com and Aliexpress.com Privacy Policy*. Retrieved 12 20, 2014, from <http://www.alibaba.com>: http://www.alibaba.com/help/safety_security/policies_rules/others/001.html
42. Amazon. (n.d.). *Transaction and Account Security*. Retrieved 12 15, 2014, from <https://payments.amazon.com>: <https://payments.amazon.com/sdui/sdui/about?nodeId=5969>
43. Andress, J. (2011). *The basics of information security*. Syngress.
44. Androidbg. (n.d.). *NFC [Near Field Communication]*. Retrieved 01 07, 2014, from <https://www.androidbg.com/>: <https://www.androidbg.com/node/361>
45. Androidcentral. (n.d.). *Staying safe with Google Wallet*. Retrieved 12 15, 2014, from <http://www.androidcentral.com>: <http://www.androidcentral.com/staying-safe-google-wallet>
46. Anton, A. E. (n.d.). *Strategies for Developing Policies and Requirements for Secure Electronic Commerce Systems. 1st Workshop on Security and Privacy in E-Commerce at CCS2000*.
47. Apple. (n.d.). *Apple Pay security and privacy overview*. Retrieved 12 01, 2014, from <http://support.apple.com>: <http://support.apple.com/en-us/HT203027>
48. Atkins, W. (2004). *The Smart Card Report*. Elsevier.
49. Baet. (n.d.). *Онлайн разплащания, Стандарт за сигурност на данните при картови разплащания*. Retrieved 04 2013, 20, from <http://baet.net/>: <http://baet.net/category/e-payments>

50. Baker, L. (2015). *The Top 12 Online Payment Alternatives to PayPal*. Retrieved from [www.searchenginejournal.com: http://www.searchenginejournal.com/top-12-alternatives-paypal](http://www.searchenginejournal.com/top-12-alternatives-paypal)
51. Basaga. (2013). *Електронна търговия*. Retrieved 03 20, 2013, from [basaga.org: http://basaga.org/wiki/index.php?title.2012](http://basaga.org/wiki/index.php?title.2012)
52. Bauknecht, K. A. (2003). *E-Commerce and Web Technologies*. Springer.
53. Bavelier, D. G. (2011). Brains on Video Games, *Nature Reviews. Neuroscience*.
54. Benjamin, R. R. (1993). *A Report by Committee of Physical, Mathematical, and Engineering Sciences. Grand Challenges 1993: High Performance Computing and Communications, Federal Coordinating Council for Science, Engineering, and Technology; Office of Science and Technology Poli*. Washington.
55. Bhasker, B. (2009). *Electronic commerce*. Tata McGraw-Hill Publishing.
56. BNB. (n.d.). *Въпроси, отнасящи се до системата RINGS*. Retrieved 06 04, 2015, from [www.bnb.bg: https://www.bnb.bg/AboutUs/AUFAQ/CONTR_PAYMENT_SYSTEM_FAQ](https://www.bnb.bg/AboutUs/AUFAQ/CONTR_PAYMENT_SYSTEM_FAQ)
57. C., P. (2005). *The Web Hosting Manager*. Lulu.com.
58. Carlson, C. (2010, 09 22). *Companies spend 5 percent of IT budget on security*. Retrieved 15 15, 2013, from [http://www.fiercecio.com: http://www.fiercecio.com/story/gartner-companies-spend-5-it-budget-security/2010-09-22](http://www.fiercecio.com/story/gartner-companies-spend-5-it-budget-security/2010-09-22)
59. CERT. (n.d.). *Computer Emergency Response team*. Retrieved 06 20, 2013, from <http://www.cert.org>.
60. Choi, S., Whinston, A., & Stahl, D. (1997). *Economics of Electronic Commerce*. Macmillan Computer Publishing.
61. Chou, T. (2012). *Information Assurance and Security Technologies for Risk Assessment and Threat management*.
62. CIO. (2002). Ролята на международните стандарти. *CIO*.
63. CIO. (2007). Одит на Информационната сигурност - обхват, стандарти, добри практик. *CIO*.
64. CIO. (2009). Внедряването на системи за управление на информационна сигурност – етапи и предизвикателства. *CIO*.
65. CIO. (2012). HP отчита двойно повече атаки и 40% повишаване на разходите, свързани с киберпрестъпления. *CIO*.
66. CIO. (2013). 4 Прогнози за мобилната сигурност. *CIO*.
67. CIO. (2013). Вътрешните заплахи - технологиите не могат сами да решат този проблем. *CIO*.
68. CIO. (2013). Информационната сигурност – 13 тенденции за 2013 година. *CIO*.
69. CISCO. (n.d.). *Wireless LAN Security, Policy, and Deployment Best Practices*. Retrieved 02 15, 2015, from [://www.slideshare.net: http://www.slideshare.net/Cisco_Mobility/wireless-lan-security-policy-and-deployment-best-practices](http://www.slideshare.net/Cisco_Mobility/wireless-lan-security-policy-and-deployment-best-practices)
70. *Comparison of Information Security Standard*. (n.d.). Retrieved 05 15, 2013, from [http://www.continuityplantemplates.com: http://www.continuityplantemplates.com/comparison-information-security-standard-iso-15048-iso-27002-nist-800-33-and-hipaa](http://www.continuityplantemplates.com/comparison-information-security-standard-iso-15048-iso-27002-nist-800-33-and-hipaa)
71. *Components of a VoIP network*. (n.d.). Retrieved 12 14, 2013, from [http://pic.dhe.ibm.com: http://pic.dhe.ibm.com/infocenter/wvraix/v6r1m0/index.jsp?topic=%2Fcom.ibm.wvraix.vqip.doc%2Fcompofvoip.html](http://pic.dhe.ibm.com/infocenter/wvraix/v6r1m0/index.jsp?topic=%2Fcom.ibm.wvraix.vqip.doc%2Fcompofvoip.html)

72. *Confidentiality, Integrity & Availability*. (n.d.). Retrieved 05 27, 2013, from <http://ishandbook.bsewall.com>:
<http://ishandbook.bsewall.com/risk/Methodology/CIA.html>
73. CRC.bg. (n.d.). *Регистър на доставчиците на удосверителни услуги*. Retrieved 02 10, 2015, from <http://crc.bg>: <http://crc.bg:8080/dpls/apex/f?p=923:310>:
74. Daniel, P. (2003). *Information Security Management Version 1. European workshop on industrial computer systems*. Marconi Selenia Secure Systems. Liverpool.
75. Darkfinance.bg. (n.d.). *България минава на електронни разплащания*. Retrieved 03 02, 2015, from www.darikfinance.bg.
76. Davidson, J. P. (2007). *Voice Over IP Fundamentals*. Cisco Press.
77. Davies, J. (2011). *Implementing SSL / TLS Using Cryptography and PKI*. Wiley Publishing.
78. Dhotre, I. .. (2010). *Information Security*.
79. Dong, L. C. (2012). *Cryptographic Protocol: Security Analysis Based on Trusted Freshness*. Springer.
80. Douligeris, C. N. (2007). *Network Security: Current Status and Future Directions*. IEEE Press.
81. Ebay. (n.d.). *Ebay Safety center*. Retrieved 11 15, 2014, from <http://pages.ebay.co.uk>:
<http://pages.ebay.co.uk/safetycentre/eBaybp.html>
82. Ebizmba. (2012). *Top 15 Most Popular Social Networking Sites*. Retrieved from <http://www.ebizmba.com/>: <http://www.ebizmba.com/articles/social-networking-websites>
83. Ec-Council. (2010). *Network Defense: Perimeter Defense Mechanisms*. Cengage learning.
84. Ecommercenews.eu. (n.d.). *Key ecommerce trends in 2015*. Retrieved 01 05, 2015, from <http://ecommercenews.eu>: <http://ecommercenews.eu/key-e-commerce-trends-in-2015>
85. Econ.bg. (n.d.). *Дебитните и кредитните карти вече са неизменна част от живота на българите*. Retrieved 04 02, 2015, from www.econ.bg.
86. Economy.bg. (n.d.). *Българите масово се страхуват за сигурността си в Интернет*. Retrieved 03 21, 2013, from <http://www.economy.bg/>:
<http://www.economy.bg/bulgaria/view/4511/2011>
87. Econt. (n.d.). *Еконт партньори*. Retrieved from <https://www.econt.com>:
<https://www.econt.com/partners>
88. Epay.bg. (n.d.). *Epay*. Retrieved 11 20, 2014, from <https://www.epay.bg>:
<https://www.epay.bg>
89. Eurox-bg. (n.d.). *Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Изисквания*. Retrieved 02 11, 2013, from <http://www.eurox-bg.com>:
<http://www.eurox-bg.com/info.php?info=189&stranica=menu>
90. Fisch, E. A. (2000). *Secure Computers and Networks: Analysis, Design, and Implementation*. CRC Press.
91. Fiserveys. (2007). *2007 Consumer Bill Payment Trends Survey: Volum of Electronic Peymants*.
92. Ghannam, J. (2011). *Social Media in the Arab World: Leading up to the Uprisings of 2011*. Retrieved from <http://cima.ned.org>: http://cima.ned.org/sites/default/files/CIMA-Arab_Social_Media-Report%20-%2010-25-11.pdf
93. Gibson, D. (2011). *Managing Risk in Information Systems*.
94. Glaessner, T. K. (2002). *Electronic Security Risk Mitigation in Financial Transactions*.
95. Google. (n.d.). *Google Wallet Fraud Protection*. Retrieved 12 05, 2014, from <https://www.google.com>: <https://www.google.com/wallet/stay-safe>

96. Grant, I. (2010). *Top 10 IT Security Trends for 2011*. Retrieved 08 05, 2015, from www.computerweekly.com.
97. Gupta, P. C. (2006). *ATA COMMUNICATIONS AND COMPUTER NETWORKS*. PHI.
98. Halapacz, T. (2011). *Wireless LAN Security*. Computer Science.
99. Hannagan, T. (2008). *Management: Concepts & Practices*. Pearson Education Limited.
100. Hightechbg.com. (n.d.). *Автоматични информационни системи – рискове и заплахи към софтуера*. Retrieved from <http://www.hightechbg.com>: <http://www.hightechbg.com/avtomatichni-informacionni-sistemi-zaplahi-software>
101. Hintzbergen, J. H. (2010). *Foundations of information security based on ISO 27001 and ISO 27002.Great Britain*. Van Haren Publishing.
102. *Information Security and Privacy in Network Environments*. (1994). DIANE Publishing Company.
103. Infosecinstitute. (n.d.). *Enterprise security*. Retrieved 5 13, 2013, from <http://resources.infosecinstitute.com/>: <http://resources.infosecinstitute.com/enterprise-security-book-chapter-1>
104. *Introduction to VoIP Security*. (n.d.). Retrieved 02 11, 2015, from <http://www.slideshare.net>: <http://www.slideshare.net/null0x00/introduction-to-voip-security>
105. Investor. (n.d.). *C CellumPay – 100% сигурност на парите ви*. Retrieved 12 21, 2014, from <http://www.investor.bg>: <http://www.investor.bg/mobilni-razplashtaniia/439/a/s-cellumpay--100-sigurnost-na-parite-vi-147265/>
106. Isaca.org. (n.d.). *Secure Electronic Transaction (SET) Protocol*. Retrieved 11 15, 2013, from <http://www.isaca.org>: <http://www.isaca.org/JOURNAL/PAST-ISSUES/2000/VOLUME-6/Pages/Secure-Electronic-Transaction-SET-Protocol.aspx>
107. ISO. (n.d.). *Intenational Organization for Standartizacion*. Retrieved 03 20, 2015, from <http://www.iso.org>: <http://www.iso.org/iso/home/standards.htm>
108. ISO. (n.d.). *ISO 19011:2011*. Retrieved 11 15, 2014, from <http://www.iso.org/>: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=50675
109. ISO. (n.d.). *ISO/IEC 27001:2013*. Retrieved 12 15, 2014, from <http://www.iso.org>: http://www.iso.org/iso/catalogue_detail?csnumber=54534
110. ISO. (n.d.). *ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management*. Retrieved 03 12, 2013, from <http://www.iso27001security.com>: <http://www.iso27001security.com/html/27002.html>
111. ISO. (n.d.). *ISO/IEC 27002:2013*. Retrieved 11 20, 2013, from <http://www.iso.org>: http://www.iso.org/iso/catalogue_detail?csnumber=54533
112. ITservices. (n.d.). *IT Services Information Security Policy for eCommerce Payment Card Applications*. Retrieved 10 15, 2014, from <https://itservices.uchicago.edu>: <https://itservices.uchicago.edu/policies/it-services-information-security-policy-ecommerce-payment-card-applications>
113. James, J. (2008). *Network Security: Know it all*. Morgan Kaufman Publishers.
114. Janczewski, L. (2000). *Internet and Intranet Security Management*. IDEA Group Publishing.
115. Kahate, A. (2013). *Cryptography and Network Security*. New Delhi: McGraw Hill Education.
116. Kauffman, R. . (2002). Economics and Electronic Commerce: Survey and Directions for Research. *International Journal of Electronic Commerce*, pp. 5–116.

117. Khusial, D. M. (n.d.). *e-Commerce security: Attacks and preventive strategies*. Retrieved 12 20, 2014, from http://www.ibm.com: http://www.ibm.com/developerworks/library/co-0504_mckegney/index.html
118. Khusial, D. R. (n.d.). *e-Commerce security: Attacks and preventive strategies*. Retrieved 12 20, 2014, from http://www.ibm.com: ttp://www.ibm.com/developerworks/library/co-0504_mckegney/index.html
119. Kim, D. S. (2012). *Fundamentals Of Information Systems Security*. Jones and Bartlett Learning.
120. King, D. L. (2009). *Electronic Commerce 2010*. Prentice Hall Press.
121. Kizza, J., M. (2011). *Computer Network Security and Cyber Ethics*. Springer.
122. Kizza, J., M. (2013). *Guide to Computer Network Security*. Springer.
123. Korper, S. E. (2001). *The E-Commerce Book (Building the E-Empire)*. Academic Press.
124. Lammie, T. (2006). *CCNA INTRO: Introduction to Cisco Networking Technologies Study Guide*. Wiley Publishing.
125. Landoll, D. (2011). *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments*. Texas: CRC Press.
126. Laudon, K. C. (2013). *E-commerce*. Pearson.
127. Laudon, K. T. (2013). *E-commerce 2013: business, technology, society*. Pearson.
128. Lex.bg. (2001, 10 6). *Закон за електронния документ и електронния подпис*. Retrieved 08 03, 2014, from <http://lex.bg/>: <http://lex.bg/laws/ldoc/2135180800>
129. Main advantages (B2C). (n.d.). Retrieved 03 15, 2013, from <http://www.configurator-database.com/definitions/configurator/main-advantages-b2c>
130. Marinova, K. (2012). Security in electronic customer relationship management systems. *SECURITATEA INFORMAȚIONALĂ 2012*.
131. Maxstead, M. (n.d.). *The Internet Security Task Force*. Retrieved 04 03, 2013, from <http://ezinearticles.com: http://ezinearticles.com/?The-Internet-Security-Task-Force&id=6608803>
132. McBee, J. E. (2010). *Mastering Microsoft Exchange Server 2010*. Sybex.
133. MehdiKhorsow-Pour. (2004). *IT- solution series: E-commerce security*. CyberTech Publishing.
134. Miller, M. (2011). *Safe buying on Ebay*. Pearson.
135. Mobb. (n.d.). *Приложение mobb*. Retrieved 10 25, 2014, from <https://www.mobb.bg>
136. Nahari, H. K. (2011). *Web Commerce Security Design and Development*. Wiley Publishing.
137. Naidu, P. (n.d.). *Basic Information Security Policy for E-commerce Industries*. Retrieved 01 05, 2015, from http://www.academia.edu: http://www.academia.edu/5058350/Basic_Information_Security_Policy_for_E-commerce_Industries
138. *Network Defense: Security and Vulnerability Assessment*. (2010). EC-Council Press).
139. Newman, A. J. (2002). *Cullen Retailing: Environment & Operations*. Singapore: Seng Lee Press.
140. Newman, R. C. (2010). *Computer Security: Protecting Digital Resources*. Jones and Bartlett Publishing.
141. Ngai, E. F. (2002). A Literature Review and Classification of Electronic Commerce Research. *nformation and Management*, pp. 415–429.
142. NSI. (2015). *Стойност на покупките и продажбите на предприятията по интернет и/или мрежи различни от интернет*. Retrieved 02 04, 2015, from www.nsi.bg

143. Ohrtman, F. (2004). *Voice Over 802.11*. Artech House.
144. Oracle. (n.d.). *Pre-Installation Security Considerations*. Retrieved 11 05, 2014, from https://oracle.com:https://docs.oracle.com/cd/E24705_01/doc.91/e24258/preinstall_security.htm#CDDJJBHC
145. Parsons, J. J. (2013). *Computer Concepts*. Cengage Learning.
146. Paypal. (n.d.). *PayPal Protection for buyers*. Retrieved 11 20, 2014, from <https://www.paypal.com/:https://www.paypal.com/cgi-bin/webscr?cmd=xpt/Marketing/popup/UAeBay-outside>
147. PayZone. (n.d.). *Онлайн плащане чрез ePay*. Retrieved 05 01, 2015, from <http://payments.resonance.bg/:http://payments.resonance.bg/methods.php>
148. PCWORLD. (2014). *Съвременни заплахи и защита за мобилните устройства. PC WORLD*.
149. Platzer, C. (2012). *Preliminary Report on Social Networks Security*. he SySSec Consortia.
150. Попов, В. Е. (2014). *Business informatics*. Свищов: АИ Ценов.
151. Powersource. (n.d.). *E-Commerce Security*. Retrieved 02 20, 2015, from <http://www.powersourceonline.com:http://www.powersourceonline.com/magazine/2009/06/e-commerce-security>
152. Privatesky. (2014). *Private Sky Secure Data Encryption Overview*. Retrieved 03 07, 2014, from <http://www.privatesky.me/:http://www.privatesky.me/private-sky-secure-data-encryption-overview>
153. Pwc. (2013). *2013 Information security breaches survey*. Retrieved 04 15, 2013, from <http://www.pwc.co.uk:http://www.pwc.co.uk/assets/pdf/cyber-security-2013-exec-summary.pdf>
154. Pwc. (2013). *The Global State of Information Security® Survey*. Retrieved 06 20, 2013, from <http://www.pwc.com:http://www.pwc.com/gx/en/consulting-services/information-security-survey/about-the-survey.jhtml>
155. Pachghare, V. K. (2009). *Cryptography and Information Security*. PHI.
156. Qarkaxhija, J. (n.d.). *E-Commerce security: Attacks and preventive strategies*. Retrieved 06 01, 2015, from http://www.academia.edu:http://www.academia.edu/2324746/E-Commerce_security_Attacks_and_preventive_strategies
157. Qin, Z. (2009). *Introduction to E-commerce*. Springer.
158. Rackspace. (n.d.). *Building Your Ecommerce Strategy*. Retrieved 01 05, 2015, from http://www.rackspace.com:http://www.rackspace.com/knowledge_center/whitepaper/building-your-ecommerce-strategy
159. Radu, C. (2003). *Implementing Electronic Card Payment Systems*. Artech House.
160. Rebollo, M. (n.d.). *E-Commerce and E-Business*. Retrieved 01 09, 2015, from <http://www.slideshare.net:http://www.slideshare.net/mrebollo/ecommerce-and-ebusiness>
161. Rittinghouse, J. R. (2004). *Wireless Operational Security*. Elsevier.
162. Rizzo, P. (n.d.). *Why EMV Isn't Enough: 3D Secure Necessary To Curb Online Fraud*. Retrieved 02 15, 2014, from <http://www.pymnts.com:http://www.pymnts.com/briefing-room/security-and-risk/EMV/2013/Why-EMV-Isn-t-Enough-3D-Secure-Necessary-To-Curb-Online-Fraud>
163. Sankar, K. S. (2005). *Cisco Wireless LAN Security*. Cisco Press.
164. SANS. (n.d.). *Securing e-Commerce Web Sites*. Retrieved 05 01, 2015, from <http://www.sans.org/:http://www.sans.org/reading-room/whitepapers/webserver/securing-e-commerce-web-sites-303>

165. Sattar, A. (2008). *VOIP: Voice Over Internet Protocol Architecture and Features*. Lulu.
166. Schiff, J. L. (2013). 15 Ways to Protect Your Ecommerce Site From Hacking and Fraud. *CIO*.
167. Schneider, G. P. (2012). *E-Business*. International edition.
168. Scientists, Y. (2012). *A Study on IT Threats and Users Behaviour Dynamics in Online Social Networks*. Retrieved from www.snfactor.com.
169. Searchsecurity. (n.d.). *Digital signature*. Retrieved 09 01, 2013, from <http://searchsecurity.techtarget.com>:
<http://searchsecurity.techtarget.com/definition/digital-signature>
170. Shahibi S., W. F. (2011). Security Factor and Trust in E-Commerce Transactions. *Australian Journal of Basic and Applied Sciences*.
171. Singh, B. (2012). *Network Security and Management*. PHI Learning.
172. Slideshare.net. (2014, 01). *Online security & encryption*. Retrieved 05 14, 2014, from <http://www.slideshare.net>: <http://www.slideshare.net/hcc79/online-security-encryption>
173. Steudler, O. A. (2000). *Cisco Network Security: Building Rock-solid Networks*. Syngress Publishing.
174. Steward, M. J. (2010). *Network Security, Firewalls, and VPNs*. Jones & Bartlett Learning.
175. Stewart, J. (2012). *CISSP: Certified Information Systems Security. Professional Study Guide*.
176. Threatanalysis. (n.d.). *Threat, vulnerability, risk*. Retrieved from <http://www.threatanalysis.com>: <http://www.threatanalysis.com/blog/?p=43>
177. Tricker, R. (2002). *ISO 9001:2000 Audit Procedures*.
178. Turban, E. K. (2012). *Electronic Commerce 2012: Managerial and Social Networks Perspectives*. Prentice Hall.
179. UBB. (n.d.). *Картови услуги:UBB 3-D secure: Сигурно плащане с карта в Интернет*. Retrieved 05 07, 2013, from <http://ubb.bg>: <http://ubb.bg/bg-BG/FCK/562>
180. Ubuntu. (2012). *Ubuntu Documentation Project. Ubuntu 10.04 Lts Server Guide*. Fultus Corporation.
181. Uky. (n.d.). *E-commerce securities*. Retrieved 01 08, 2015, from <http://www.uky.edu>:
<http://www.uky.edu/~dsianita/390/390wk4.html>
182. Urbaczewski, A. J. (2002). Electronic Commerce Research: A Taxonomy and Synthesis. *Journal of Organizational Computing and Electronic Commerce*, 263–305.
183. Vakharia, A. M. (2013). Security glitches related To e-Commerce and Their Solutions. *International Journal of Computer Application*.
184. Vermillion, W. (2003). *End-to-end DSL Architectures*. Cisco Press.
185. Vtb-bank. (n.d.). *Платежные карты Банка ВТБ (Казахстан) – новый уровень безопасности*. Retrieved 01 13, 2013, from <http://www.vtb-bank.kz>: <http://www.vtb-bank.kz/bank/news/229144>
186. Webmenshirts. (n.d.). *Secure payment*. Retrieved 01 09, 2015, from <http://www.webmenshirts.com>: <http://www.webmenshirts.com/en/secure-payment>
187. Whitman, M. H. (2009). *Principles of Information Security*. Thomson Learning.
188. Whitman, M. H. (2010). *Management of Information Security*. Cengage Learning.
189. Woland, A. (2014). Secure network access. *Network World*.
190. Yen, P. (2006). *Practical Cryptology and Web Security*. Addison Wesley.
191. Zwass, V. (1996). Electronic Commerce – structure and issues. *International Journal of Electronic Commerce*, 1(1), 3-23.

Списък на използваните съкращения

1. ЕБ - Електронен бизнес
2. ЕПС - електронен превод на средства
3. ЕТ - Електронна търговия
4. ЗМСП - Закон за малките и средните предприятия
5. ИТ - Информационни технологии
6. ИС – Информационна сигурност
7. ИКТ - Информационни и комуникационни технологии
8. МКО - Международните картови организации
9. НАП – Национална агенция за приходите
10. НОИ –Национален осигурителен институт
11. ПИК - Персонален идентификационен код
12. СЕТ – Система за електронна търговия
13. СУИС - Система за управление на информационната сигурност
14. 3DES- Triple Data Encryption Standard
15. AES - Advanced Encryption Standard
16. АН - Authentication Header
17. АLE- Annualized loss expectancy
18. АRO- Annualized rate of occurrence
19. АТМ - Asynchronous Transfer Mode
20. В2В - Business to Business
21. В2С - Business to Customer
22. ВYOD - Bring Your Own Device
23. ВYОx - Bring Your Own Anything
24. СAST 128 - Carlisle Adams/Stafford Tavares
25. СBC - Cipher Block Chaining
26. СDA - Combined Data authentication
27. СFB - Cipher feedback
28. СНАР - Challenge Handshake Protocol
29. DАR – Data at rest
30. DDA - Dynamic data authentication
31. DDOS - Distributed denial of service

32. DES - Data Encryption Standard
33. DIT –Data in transit
34. DLP - Data Loss Prevention
35. DoS - Denial of service
36. DSS - Digital Signature standard
37. EAP - Extensible Authentication Protocol
38. EBPP - Electronic bill presentment and payment
39. ECB - Electronic CodeBook
40. EDI - Electronic Data Interchange
41. EF - Exposure factor
42. ESO - European Standards Organizations
43. ESP - Encapsulating Security Payload
44. IDEA - International Data Encryption Algorithm
45. IEEE - Institute of Electrical and Electronics Engineers
46. IPsec - Internet protocol security
47. ISAKMP- Internet Security Association and Key Management Protocol
48. ISDN - Integrated Services Digital Network
49. ISMS - Information security management system
50. ISO - International Organization for Standardization
51. ISTF - Internet Security Task Force
52. ITSEC - Information Technology Security Evaluation Criteria
53. KDC - Key Distribution Center
54. LCP - Link Control Protocol
55. L2F - Layer 2 Forwarding
56. L2TP - Layer 2 Tunneling Protocol
57. MAC - Message authentication code
58. MDC - Modification detection code
59. MD4 - Message digest 4
60. MD5 - Message digest 5
61. MGCP - Media Gateway Control Protocol
62. MIT - Massachusetts Institute of Technology
63. NCP - Network Control Protocols
64. NFC - Near Field Communication

65. OFB - Output FeedBack
66. OSI - Open System Interconnect
67. P2P - Peer to peer
68. PAN - Personal area network
69. PAP - Password Authentication Protocol
70. PCI DSS - Payment Card Industry Data Security Standard
71. PIN - Personal Identification Number
72. PPPoE - Point to Point Protocol over Ethernet
73. PPP - Point to Point Protocol
74. PPTP - Point-to-Point Tunneling protocol
75. PUP - Potentially unwanted program
76. RADIUS - Remote Address Dial-In User Service
77. RC5- Rivest Cipher
78. RFC - Request for Comments
79. SBU - Subtle but unclassified
80. SDA - Static data authentication
81. SET - Secure electronic transaction
82. SHA - Secure Hash Algorithm
83. SHTTP - Secure Hyper Text Transport Protocol
84. SIP - Session Initiation Protocol
85. SLE - Single loss expectancy
86. S/MIME - Secure Multipurpose Internet Mail Extensions
87. SMTP - Simple Mail Transfer Protocol
88. SOCKS - Socket Security
89. SSH - Secure Shell
90. SSL - Secure Sockets Layer
91. SWAP - Shared Wireless Access Protocol
92. TCSEC - Trusted Computer System Evaluation Criteria
93. TCP - Transmission Control Protocol
94. TKIP - Temporal Key Integrity Protocol
95. TLS - Transport Layer Security
96. TOE - Target Of Evaluation
97. TSYS - Total System Services

- 98. VoIP - Voice over internet protocol
- 99. UDP - User Datagram Protocol
- 100. URL - Uniform Resource Locator
- 101. VPN - Virtual Private Network
- 102. WEP - Wired Equivalent Privacy
- 103. WPA - Wi-Fi Protected Access
- 104. XML - Extensible Markup Language
- 105. XMPP - Extensible Messaging and Presence Protocol

Приложения

Приложение 1

Анкетна карта за проучване

Базова информация за организацията

1. Идентификация на организацията съгласно Закона за малки и средни предприятия

1.1. Брой на персонала.

- < 10
- < 50
- < 250
- > 250

1.2. Годишен оборот.

- ≤ 3 900 000 лв.
- ≤ 19 500 000 лв.
- ≤ 97 500 000 лв.
- > 97 500 000 лв.

1.3. Стойност на активите (по балансова стойност).

- ≤ 3 900 000 лв.
- ≤ 19 500 000 лв.
- ≤ 84 000 000 лв.
- > 84 000 000 лв.

1.4. Наименование на организацията, град, Web сайт:

2. Какъв модел за електронна търговия използвате?

- Електронен магазин**
- Електронни търгове**
- Електронен мол** (съвкупност от електронни магазини, които се обединяват от обща инфраструктура и търговска марка)
- Използване на търговско пространство на други организации** (използване общите възможности като търговска марка, системи за заплащане, логистика, системи за поръчки, сигурни транзакции и др.)
- Виртуални общности** (развива се от клиентите и партньорите на виртуална организация, които добавят своята информация)
- Доставчици на услуги с добавена стойност** (компаниите, които са специализирани в различни функции: електронни заплащания, логистика, сигурни транзакции и др.)
- Интегратори на добавена стойност** (За интегриране на повече стъпки от веригата за добавяне на стойност. Печалбата за продавача идва от таксите за консултации и таксите за осъществяване на транзакциите.)

Платформи за сътрудничество (набор от средства и инструменти за сътрудничество и коопериране между организациите)

Информационни брокери (предоставяне на условия за търсене на информация, издаване на информационни бюлетини, класификация на стоки и дейности, инвестиционни съвети и др.)

3. В коя от следните области извършвате електронна търговия?

- Продажба на стоки
- Продажба на услуги
- Други

Стратегия и процедури за сигурност и контрол

4. Информационната сигурност има следния приоритет за висшия мениджмънт на Вашата организация или за директора на подразделението?

- Много висок приоритет
- Висок приоритет
- Нисък приоритет
- Не е приоритет

5. Кои от следните политики и процедури за сигурност, са разработени във Вашата организация?

- Практиките на персонала
- Оторизиране използването на мрежови услуги
- Използване на корпоративния e-mail, интранет и Интернет
- Управление на паролите
- Придобиване на софтуер и хардуер
- Политика и стандарти на криптиране
- Отговор и управление на инциденти свързани със сигурността
- Политика за управление на данните (която да включва използване на данните, съхраняване и унищожаване на чувствителни данни)
- Отдалечен достъп до мрежата на организация

6. Как оценявате степента на конфиденциалност на данните, с които работите през Интернет?

- Високо конфиденциални
- Конфиденциални
- Не са конфиденциални

7. Сертифицирана ли е Вашата организация по стандарта ISO 27001?

- Да
- Планираме сертифициране в следващите 12 месеца
- Не

8. Платформата за електронна търговия, която използвате е:

- Разположена на собствен сървър, администриран от персонала на организация
- Разположена на външен сървър на доставчик на услуги
- Друго, моля уточнете: _____

Инвестиране в информационната сигурност

9. Коя е главната причина за направените от Вас разходи за информационна сигурност?

- Защита на различните активи от кражба
- Повишаване на ефективността
- Предоставяне на нови бизнес възможности
- Защита на интелектуалната собственост
- Поддържане на бизнеса в ситуация на бедствие
- Поддръжка на интеграцията на данните
- Защита на репутацията на организацията
- Придържане към законите и наредбите
- Предотвратяване на престопите и прекъсванията
- Други

10. Каква част от бюджета за ИТ се изразходва за информационна сигурност?

- Няма разходи за информационна сигурност
- 1 % или по-малко
- Между 2% и 5%
- Между 6% и 10%
- Между 11% и 25%
- Повече от 25%

11. Как измервате ефективността на разходите за информационна сигурност?

- Измерване на тенденциите в сигурността – инциденти/разходи
- Сравнителен анализ с други организации
- Изчисления за възвръщаемост на инвестициите (ROI)
- Измерване на информираността на персонала
- Мониторинг на нивото на спазване на нормативната уредба
- Обратна връзка от управлението
- Друг формализиран процес
- Официално не оценяваме ефективността на разходите за информационната сигурност

Нарушения в сигурността

12. В последната година имали ли сте инциденти в сигурността?

- Не сме имали инцидент в сигурността
- Имали сме някакъв инцидент в сигурността
- Имали сме случаен инцидент в сигурността
- Имали сме зловреден инцидент в сигурността
- Имали сме сериозен инцидент в сигурността

13. Какъв тип инциденти в сигурността сте имали?

- Не сме имали
- Авария в системите или увреждане на данни
- Инфекция с вируси или зловреден софтуер

- Кражба или измами, чрез използване на ИТ
- Други инциденти, причинени от персонала
- Атаки от неупълномощено външно лице (включително хакерски опити)

Физическа сигурност

Моля да отговорите на въпроса, само ако приложението за електронна търговия е разположено на собствен сървър, който е администриран от персонала на организацията.

14. Какъв тип на контрол на периметъра прилагате към достъпа до централите за данни?

- Чипове/карти
- Контрол чрез пароли въвеждани с клавиатура
- Биометрични контроли
- Охрана

Моля да отговорите на въпроса, само ако приложението за електронна търговия е разположено на собствен сървър, който е администриран от персонала на организацията.

15. Наблюдавате ли/записвате ли целия достъп до центъра с данни?

- Да
- Не

Администрация на сигурността на информацията

Моля да отговорите на въпроса, само ако приложението за електронна търговия е разположено на собствен сървър, който е администриран от персонала на организацията.

16. Ограничавате ли нивото на достъпа на администратора на мрежовата и системната инфраструктура?

- Да
- Не

Моля да отговорите на въпроса, само ако приложението за електронна търговия е разположено на собствен сървър, който е администриран от персонала на организацията.

17. Какъв е средният трудов стаж на персонала, занимаващ се с информационната сигурност?

- от 1 до 3 години
- от 3 до 5 години
- над 5 години

Моля да отговорите на въпроса, само ако приложението за електронна търговия е разположено на собствен сървър, който е администриран от персонала на организацията.

18. Контролира ли се строго достъпа до дневниците за сигурността (дневници на защитната стена и др.)?

- Да
- Не

Защитна стена (firewall) и откриване/предотвратяване на нарушенията

19. Имате ли екип по сигурността, който да следи за известните заплахи?

- Да
- Не

20. Имате ли екип за реагиране при инциденти?

- Да
- Не

21. Използвате ли сървър/и на защитната стена за защита на вашата мрежа?

- Да
- Не

22. Сканирате ли и проверявате ли всички допустими услуги, предоставяне от вашия сървър на защитната стена?

- Да
- Не

23. Имате ли инструменти за отчитане и анализиране на дневниците (log) на защитната стена?

- Да
- Не

24. Имате ли документирана и проверена политика за сигурност на защитната стена?

- Да
- Не

Контрол за зловреден софтуер

25. Сканирате ли всички е-майл съобщения за вируси?

- Да
- Не

26. Имате ли централизирано администриране на контрола на вирусите, като например разпространение на обновяванията на сигнатурите, докладване, политика за прилагане и управление от доставчика?

- Да
- Не

27. Позволявате ли инсталация на личен и неодобрен от корпорацията софтуер на мрежовите компютри?

- Да
- Не

Мониторинг

28. Наблюдавате ли сигурността/нарушения и наличните приложения/мрежови услуги?

- Да
- Не

29. Записвате ли в дневници успешните и неуспешните опити за достъп?

- Да
- Не

Приложение 2

Таблица 2.9.

Сравнение на протоколите за информационна сигурност

Протокол	Критерий 1 (разработен от)	Критерий 2 (ниво, на което се използва)	Критерий 3 (приложимост)	Критерий 4 (функция)	Критерий 5 (RFC дефиниция)	Критерий 6 (стабилност)	Критерий 7 (съвместимост)	Критерий 8 (криптиране)
<i>Протоколи за удостоверяване</i>								
1. One-Time Password System S/Key	Bellcore	Мрежово ниво	<input checked="" type="checkbox"/>	Генериране на еднократни пароли	1760	Стабилен за съвременни десктоп и мобилни устройства	Linux	Hash функции
2. PPP	Internet Engineering Task Force (IETF)	Канално ниво	<input checked="" type="checkbox"/>	Удостоверяване	1661	Стабилен за съвременни десктоп и мобилни устройства	Windows, Linux	Базово
3. TACACS +	Bolt, Beranek and Newman (BBN), Cisco Systems	Приложно ниво	<input checked="" type="checkbox"/>	Удостоверяване	927	Стабилен за съвременни десктоп и мобилни устройства	Unix, Windows NT	Базово

4. RADIUS	Livingston Enterprises Inc.	Приложно ниво	<input checked="" type="checkbox"/>	Удостоверяване, оторизация, отчетност	2865	Стабилен за съвременни десктоп и мобилни устройства	Unix, Windows NT	Hash функции
5. KERBR OS	Massachusetts Institute of Technology (MIT)	Мрежово ниво	<input checked="" type="checkbox"/>	Удостоверяване чрез доверена трета страна	1510	Стабилен за съвременни десктоп и мобилни устройства	Windows, Mac OS, Linux, Z/OS	Data encryption standard (DES)
6. FORTEZ ZA	NSA	Мрежово ниво	<input checked="" type="checkbox"/>	Идентификация, удостоверяване, конфиденциалност, цялост		Стабилен за съвременни десктоп и мобилни устройства	Windows, Unix	Високо ниво с алгоритми KEA и SKIP-JACK
<i>Протоколи в слоевете на модела OSI</i>								
7. SHTTP	Eric Rescorla and Allan M. Schiffman	Приложно ниво	<input checked="" type="checkbox"/>	Комуникация със защитени съобщения	2660	Стабилен за съвременни десктоп и мобилни устройства	Windows	Базово
8. S/MIME	RSA Data Security, IETF	Приложно ниво	<input checked="" type="checkbox"/>	Защита на електронна поща	3369,3370,3850,3851	Стабилен за съвременни десктоп и мобилни устройства	Windows	Чрез набор от стандарти PKCS

9. SSL	Netscape	Транспортно ниво	<input checked="" type="checkbox"/>	Криптиране, удостоверяване, цялост	6101	Стабилен за съвременни десктоп и мобилни устройства	Windows, Mac OS, Linux	Чрез 3DES
10. TLS	IETF	Транспортно ниво	<input checked="" type="checkbox"/>	Криптиране, удостоверяване, цялост	5246	Стабилен за съвременни десктоп и мобилни устройства	Windows, Mac OS, Linux	CipherSuites-шифър и hash функция
11. SSH	SSH Communication s Security Ltd	Транспортно ниво	<input checked="" type="checkbox"/>	Защитено отдалечено влизане	4250, 4251, 4252, 4253, 4254	Стабилен за съвременни десктоп и мобилни устройства	Windows, Mac OS, Linux, OS/2	Солидно криптиране
12. SET	Mastercard & Visa	Транспортно ниво		Криптиране, автентификация, конфиденциалност	3538		Windows, Linux	Солидно криптиране
13. SOCKS	David and Michelle Koblas	Транспортно ниво	<input checked="" type="checkbox"/>	Мрежова защитна стена	1928	Стабилен за съвременни десктоп и мобилни устройства	Windows, Linux	
14. IPsec	IETF	Мрежово ниво	<input checked="" type="checkbox"/>	Криптиране, автентификация, капсуловане	2401, 2402, 2406, 2408	Високо надежден и стабилен	Windows, Mac OS, Android, iOS	Най-високо ниво с цифрови сертификати
15. L2F	Cisco Systems	Канално ниво		Тунелиране	2341	Стабилен за съвременни десктоп	Windows, Linux, Mac OS	

						и мобилни устройства		
16. PPTP	Microsoft	Канално ниво	<input checked="" type="checkbox"/>	Тунелиране	2637	Стабилен за съвременни десктоп и мобилни устройства	Windows, Linux, MAC OS	Базово
17. L2TP	Cisco ,Microsoft	Канално ниво	<input checked="" type="checkbox"/>	Тунелиране	2661	Високо надежден и стабилен	Windows, Linux, MAC OS	Най-високо ниво с цифрови сертификати
18. PPPoE	UUNET, Ericsson, Wind River Systems	Канално ниво	<input checked="" type="checkbox"/>	Капсулиране	2516	Стабилен за съвременни десктоп и мобилни устройства	Windows, Linux, MAC OS	Базово
<p><i>Протоколи при виртуални частни мрежи</i> Използваните протоколи за VPN са L2F, PPTP, L2TP и IPsec и вече бяха представени в таблицата</p>								
<p><i>Протоколи при безжични мрежи</i></p>								
19. WEP	IEEE	Канално ниво		Криптирана комуникация			Windows, Linux, MAC OS	Алгоритъм RC4

20. TKIP	IEEE	Канално ниво	<input checked="" type="checkbox"/>	Криптирана комуникация		Стабилен за съвременни десктоп и мобилни устройства	Windows, Linux, MAC OS	Алгоритъм RC4
21. EAP-TLS	IETF	Транспортно ниво	<input checked="" type="checkbox"/>	Електронни сертификати за удостоверяване	2716	Стабилен за съвременни десктоп и мобилни устройства	Windows, Linux, MAC OS	Базирано на TLS
22. EAP-TTLS	Funk Software, Certicom	Канално ниво	<input checked="" type="checkbox"/>	Удостоверяване с допълнителна информация	5281	Стабилен за съвременни десктоп и мобилни устройства	Windows, Linux, MAC OS	Базирано на TLS
23. LEAP	Cisco	Транспортно ниво	<input checked="" type="checkbox"/>	Удостоверяване на база обща тайна		Стабилен за съвременни десктоп и мобилни устройства	Windows, Linux, MAC OS	Базово
24. PEAP	Cisco, Microsoft, RSA security	Транспортно ниво	<input checked="" type="checkbox"/>	Удостоверяване с електронни сертификати		Стабилен за съвременни десктоп и мобилни устройства	Windows, Linux, MAC OS	Базово
<p><i>Протоколи при Voice over (VoIP) мрежи</i></p>								

25. H.323	International Telecommunication Union (ITU)	Транспортно ниво	<input checked="" type="checkbox"/>	Договаряне на защитните механизми		Стабилен за съвременни десктоп и мобилни устройства	Windows, Linux, MAC OS	Базово
26. SIP	IETF	Приложно ниво	<input checked="" type="checkbox"/>	Удостоверяване, конфиденциалност, запазване целостта на съобщенията	3261	Високо надежден и стабилен стандарт за VoIP	Windows, Linux, MAC OS	Базово