УНИВЕРСИТЕТ ПО БИБЛИОТЕКОЗНАНИЕ И ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

КАТЕДРА ”ИНФОРМАЦИОННИ СИСТЕМИ И ТЕХНОЛОГИИ”
СПЕЦИАЛНОСТ «ИНФОРМАЦИОННИ ТЕХНОЛОГИИ И ФИНАНСОВ ИНЖЕНЕРИНГ»

МАГИСТЪРСКА ТЕЗА

на тема:

АНАЛИЗ НА ИНФОРМАЦИОННИ СИСИТЕМИ ЗА ФИНАНСОВИ ИНСТИТУЦИИ И ИНТЕРНЕТ СИГУРНОСТ

Дипломант:
Николай Колев
задочно обучение
Ф.№ 015-ФИЗ

Научен ръководител:.....
(Проф. д.н. И. Гарванов)

София
2016

РЕЗЮМЕ НА МАГИСТЪРСКАТА ТЕЗА

Колев, Николай Добринов 015-ФИЗ
Заглавие: АНАЛИЗ НА ИНФОРМАЦИОННИ СИСИТЕМИ ЗА ФИНАНСОВИ ИНСТИТУЦИИ И ИНТЕРНЕТ СИГУРНОСТ
Проф. д.н. Иван Ганчев Гарванов, ръководител катедра „Информационни системи и технологии“ 2016, София
„Информационни системи и технологии“ / Университет по Библиотекознание и Информационни технологии
Брой на страници: 104
Брой на цитирани и използвани източници: 12
Брой на приложения, графики, илюстрации и др.: 20 фигури + 2 Таблици
Цели на магистърската теза са, изложени в резюмето представено по долу.
Ключови думи: информационна система, електронно банкиране, системи за сигурност

Избраната тема за Магистърската теза е „Анализ на информационни системи за финансови институции и интернет сигурност“. Нейната основна цел е да изясни понятието Информационна система, видовете Информационни системи, основни термини свирзани с тях, етапите им на развитие, както и обвързаността им с Интернет сигурноста, Електронните разплащания и Електронното банкиране. Магистърската теза обхваща основните понятия за информационна сигурност и информационна система. Спира се по подробно на целите, изискванията и категориите информационна сигурност.

Магистърската теза представя системния подход към информационната сигурност и нейната структура. Също така са разгледани някои базови характеристики и обвързаността на информационната сигурност и бизнеса. В тезата са разгледани трите основни нива на информационна сигурност Базово, Средно и Високо ниво на информационна сигурност. Застъпено е по-подробно интернет банкирането, както и методите за сигурност свързани с него. Разгледана е системата и спецификата на безконтактните плащания, както и тяхната специфика, проблеми и сигурност.

Представени са някои заплахи и възможни защити при извършване на този вид он лайн дейности. Като основни модели за сигурност при интернет банкирането и други видове он лайн операции свързани с финансите са разгледани по подробно методите за уеб сигурност, криптиране и декриптиране на данни. Електронния подпис и Токен устройствата, които представляват отделен хардуер свързан със сигурноста на он лайн банкирането и други видове он лайн финансови операции.

СЪДЪРЖАНИЕ

УВОД

В информационната ера електронното плащане започва да става все по-важно. Бяха въведени нови финансови процедури и монетарни структури, които да рефлектират на технологичните възможности и изискванията на съвременната икономика. Глобализацията и Интернет промениха начина по който крайните потребители и компаниите извършват своите разплащания. При традиционното плащане, определена стойност се прехвърля по няколко различни начина - документно или в брой. Разплащането в брой използва банкноти и монети, които се издават под контрола на правителствата. Документните плащания използват ордери, чекове, пощенски трансфери, акредитиви и банкови карти.

Различните методи за разплащане имат различни свойства. Те варират от пълна анонимност при плащанията в брой до пълна идентификация при плащанията с банкови карти. Различните транзакции могат да бъдат проследени в различна степен, а таксите за транзакциите са различни в зависимост от метода за разплащане. Причината за съществуването на толкова много механизми е, че съществуват различни обстоятелства - това дава на всеки механизъм пазарна ниша.

Както при традиционните методи за разплащане, така и електронните най-големия проблем е да бъде осигурено, че никой няма да може да копира цифровите пари и, че никой няма да може да открадне информацията за кредитната карта. Финансовите транзакции между отделните банки отдавна бяха приведени в електронен вид. SWIFT (Society for World-Wide Interbank Financial Telecommunication - общество за международни междубанкови финансови телекомуникации)" мрежата представлява частна мрежа, която напоследък се свързва към публични мрежи, като Интернет.

За да могат да емулират характеристиките на съществуващите схеми за разплащане, електронните системи за разплащания трябва да отговарят на определени изисквания. Системите за Интернет плащания трябва да бъдат много гъвкави - те трябва да поддържат различни модели на плащания за различни ситуации (примерно плащане чрез кредитна карта, в брой или чек). Периодът за плащането трябва да бъде договорен между двете страни.

Системите трябва да позволяват извършването на конверсия на цифровите пари от една в друга система за разплащане. Инфраструктурата за разплащане трябва да поддържа множество форми на разплащания, различни цифрови валути и освен това е необходимо сключването на договори с други доставчици на цифрови и реални финансови услуги - това ще позволи конвертирането на паричните средства в други системи.

За да има успех дадена инфраструктура за разплащане, тя трябва да бъде достъпна и добре приета от всеки. Потребителите трябва да имат възможност да ограничат своите загуби чрез въвеждането на минимален резерв или на максимална допустима сума за еднократно плащане - при надхвърлянето на тези лимити трябва да е необходимо допълнително потвърждение, преди извършване на плащането. Следенето на плащанията трябва да може да се извършва лесно. Инфраструктурата трябва е такава, че всеки да може да я използва без посредник (примерно банка).

Интернет може да поеме всички финансови транзакции, но поради защитни причини е необходимо използването на съществуващите финансови къщи за клиринг. Всяка транзакция включва купувач и продавач на продукти, информация или услуги. За всяка финансова транзакция е необходима и финансова институция, която да извърши паричния трансфер, дори в повечето случаи са необходими две финансови институции (на продавача и купувача). Електронното разплащане започва с комуникация между купувача и неговата финансова институция, при която купувача и нарежда да извърши плащане (примерно чрез изтегляне на средства от банкова сметка или от кредитната карта). След това парите се изпращат за клиринг към финансовата институция на продавача. Ако тя валидира парите, продавача ще получи потвърждение за плащането. След това, той може да започне да обработва поръчката.

Най-важният проблем на цифровите системи за разплащания е сигурността. Тъй като плащанията са с реални пари, системите за цифрови разплащания са основната цел на криминалния контингент във всички страни по света. В реалния свят, копирането на банкноти е трудно, но не и невъзможно, стига да е налице необходимото оборудване. Все пак, фалшифицирането на реалните пари отнема време и средства, а и съществува голяма

вероятност банката да открие фалшификацията. В Интернет цените за копиране са почти нулеви, промяната на серийни номера е елементарно. Следователно трябва да се гарантира, че системата е защитена, в противен случай тя няма да се приеме от потребителите. Интернет е отворена мрежа, позволяваща на всеки да следи трафика на останалите - следователно съобщенията трябва да бъдат защитени от модифициране чрез използване на цифров подпис. Друг важен проблем е осигуряването, че парите ще достигнат до желаното местоположение. Примерно, когато плащате в магазин, давате парите на продавача (или касиера), но когато плащате през Интернет съществува възможност плащането да пристигне в друга банкова сметка, без това да бъде забелязано. Следователно за осигуряване защитата на финансовите транзакции са необходими специализирани технологии.

За да позволи извършването дори на минимални по стойност плащания, системата не бива да създава допълнителни разходи и да влошава своята производителност. В реалния свят за да позволи плащания с кредитни карти, търговеца дължи около 4% от транзакцията на финансовите институции - това прави разплащанията с кредитни карти неприложими за малки суми.

След като получите цифровите си пари, трябва да имате възможност да ги внесете в банка или пък да ги съхраните. Това изисква тези пари да бъдат приемани навсякъде, по същия начин както кредитните карти или реалните пари. Това приемане трябва да е такова, че дори да е приемливо за хора, които не използват Интернет. Интернет транзакциите трябва да бъдат конфиденциални. Това налага защитата от трети страни, които биха желали да проникнат в транзакцията и дори ако те успеят да проникнат в нея да не могат да я прочетат (тъй като се използва кодиране). Съобщението от купувача към продавача трябва да бъде подписано за да гарантира, че никой друг няма да може да изтегли пари от сметката или кредитната карта на купувача без негово съгласие. Всяко съобщение трябва да бъде уникално - това ще гарантира уникалността на всяка финансова транзакция. След завършването на транзакцията, продавача изпраща потвърждение на купувача.

Финансовата система трябва да бъде достъпна и надеждна. Прекъсването или блокирането на инфраструктурата означава загуба за всички участници. Всеки участник трябва да може да завърши своята част от транзакцията, когато пожелае или когато му е необходимо. Една транзакция никога не бива да остава в незавършено състояние - плащането или се приема, или се отхвърля, но никога не остава в неустановено състояние. Неустановеното състояние означава възможност за загуба на парите в Интернет. Протоколът за разплащане трябва да следи и обработва случаите, когато мрежата или някой от участващите компютри претърпи срив. Обикновено в тези случаи цялостната транзакция става невалидна и действията по нея следва да бъдат повторени, но някои системи позволяват продължаването от точката на спиране на транзакцията.

Наподобяващите плащане в брой системи трябва да поддържат гарантиране на анонимност и непроследимост на транзакцията, тъй като това са основните предимства на реалното плащане в брой Това може да се постигне само ако за транзакцията не е необходимо присъствието на трета страна. Анонимността позволява скриване идентичността на потребителя, а непроследимостта не бива да позволява свързване на различните плащания на един потребител (не бива да се следят пазарните навици на потребителя, нито източниците на неговите доходи). Това може да се постигне чрез кодиране на всички обменяни съобщения. Все пак, анонимността се запазва най-добре, когато цената за проследяване на дадена транзакция е по-голяма от стойността на придобитата чрез това проследяване информация.
С разрастването на Интернет се увеличава и необходимостта от системи за разплащане. Тези системи трябва да могат да се справят с нарастващия брой потребители и търговци, без да влошат своята производителност. Поради това се предпочитат разпределените системи, при които сървърите за разплащане се намират на различни места в Интернет - това осигурява както производителност, така и надеждност в случаите на отпадане на даден сървър или мрежови сегмент.

Инфраструктурата за плащания трябва да поддържа съществуващите Интернет приложения чрез програмен интерфейс, така че да не е необходимо модифицирането на тези приложения.

Глава 1. ИНФОРМАЦИОННА СИСТЕМА - Понятие, термини, етапи на развитие

Информационна система е комбинация от информационни технологии и действия на хората, които ги прилагат за управлението на процеси, вземане на решения и др. с помощта на компютърни системи. Системата е предназначена за използване от организация или физическо лице и дава възможност за съхранение на бази данни, управление и обработка на цялата информация или на част от нея. [1]

Съществуват различни информационни системи: финансови, промишлени, географски и др. Като цяло информационните системи могат да бъдат разделени на такива, предназначени да извършват определена операция (обработка на транзакции, Transaction Processing) и на такива, които са предназначени за събиране на данни, необходими при вземането на решения (Decision Support).

Според това на какво ниво в организацията се ползват, информационните системи могат да бъдат разделени на четири нива, които отдолу нагоре са:

Системи за обработка на транзакциите – ползвани основно от оперативните работници. Това са всички системи, които се използват в ежедневната работа на специфична компания, било то географска информационна система, системи за CAD, графично оформление и онлайн публикуване, подпомагане на телефонни услуги и др.

Управленски (или мениджърски) информационни системи – ползвани от оперативния мениджмънт. Примери са системите за управление на взаимоотношенията с клиентите (CRM), за планиране на ресурсите на предприятието (ERP), системите и за управление на съдържанието.

Системи за подпомагане на решения – системи за подпомагане на колективното управление и взимане на решения. Подобни приложения са групуер системите.

Директорски информационни системи – предоставят редовни отчети и информация за прогреса по работата в организацията.

Фиг.01 Класифицираща пирамида на различни информационни системи според нивото им в организационната йерархия.

В заключение можем да дадем следното най-обобщено определение от управленска гледна точка. Информационна система е средство, което обхваща всички форми на събиране, съхраняване, извличане, обработка и разпространение на информация. Тя е множество от

взаимосвързани компоненти, което доставя информационни услуги и подпомага процеса на вземане на решения, координацията и контрола в рамките на организацията. Разликата между понятията "информационна система" и "информационни технологии" е съществена. Терминът "информационни технологии" обхваща различните средства (хардуер, софтуер, за управление на данните), които са необходими за функционирането на дадена система. [4]

С други думи информационна система обединява всички видове информационни дейности. В допълнение тя съдействува на мениджърите и служителите при анализирането на проблеми и създаването на нови продукти. Тя съдържа данни за хора, места и обекти, значими за съответната организация. В информационната система се наблюдават три основни дейности, които служат за произвеждане на информация: въвеждане, обработка и извеждане. Въвеждането обхваща и събира необработените данни в рамките на организацията и нейната обкръжаваща среда. Обработката преобразува данните в значима информация. Извеждането прехвърля информацията на хората, за да подпомогне техните дейности. Информационната система се нуждае от обратна връзка, т.е. от външни данни, чрез които да се оцени коректността на въвеждането.

Следователно информационна система също може да се разглежда като специфична бизнес система, чийто бизнес процес обхваща събиране, предаване, съхраняване, извличане, обработка и извеждане на информация. Софтуерните продукти и електронните таблици не се считат за информационни системи, понеже от своя страна те не отговарят на дефиницията за бизнес системи.

От гледна точка на бизнеса информационните системи следва да се разглеждат като организационно и управленско решение, използуващо информационни технологии. Тяхното прилагане изисква детайлното познаване на дадена организация заедно с нейните основни характеристики: човешки ресурси, структура, оперативни процедури, политики и култура. [2]

Основно изискване към всяка информационната система е да осигурява и поддържа интегриран информационен поток в рамките на дадена организация, така че във всеки един момент от време, всеки, който се нуждае, да може да получи необходимите му сведения.

Информационната система се дефинира чрез функциите, които предоставя на своите потребители. Нейна основна цел е да събира, съхранява, обработва и разпространява информация.

Като всяка система, тя се изгражда от отделни компоненти или подсистеми и притежава специфична архитектура. Под архитектура се разбира интегрирания структурен проект на дадена система. Тя обхваща отделните елементи на системата, техните взаимодействия и начина на тяхното функциониране.

1.1.Компоненти на Информационната система

Архитектурата на информационната система предполага две основни дейности:

- моделиране на данните и процесите в организацията;
- представяне на бизнеса на организацията чрез модела;

Всяка организация контролира дейността си чрез структурирана йерархия и формални, стандартни процедури. Йерархията класифицира хората и ги подрежда възходящо по отговорности и права. Стандартните оперативни процедури представляват формални правила, които са разработени с течение на времето за извършване на определени дейности при настъпването на определени ситуации.

Всяка информационна система включва следните базови компоненти, които във взаимодействие помежду си реализират процес на трансформация на входни данни в изходна информация, необходима на заинтересованите страни за реализация на конкретни цели.

Хардуер: Терминът хардуер ни насочва към машинната част на информационната система. Тази категория включва самият компютър, който често се нарича централен процесор (CPU) и всички негови инструменти за поддръжка. Сред инструментите за поддръжка са входните и изходните устройства, устройствата за съхранение на информацията и комуникационните устройства.

Софтуер: Терминът софтуер ни насочва към компютърните програми и ръководствата(ако има такива), които ги поддържат. Комютърните програми са инструкциите, които могат да се четат от машината, и могат за управляват веригите в хардуерната част на системата по такъв начин, че да получава важна информация от данни. Програмите често се съхраняват на някаква входна/изходна среда, като например диск, преносим хард диск или флаш памет.

Данни: Данните са фактите, които се използват от програмите, за да получи важна информация, данните често се съхраняват под някаква форма, която може да бъде използвана по-късно от машината. Например диск, преносим хард диск или флаш памет.

Процедури: Процедурите са политиката, която следва компютърната система. Една аналогия, по която често се използва, за да покаже ролята на процедурите в системата, е "Процедурите за хората са като програмите за машината ".

Хора: Всяка система се нуждае от хора, ако иска да е полезна. Много често най-пренебрегнатата част от системата са хората, въпреки, че те са тези, които играят най-важна роля в успеха или провала на информационната система. Това включва не само потребителите, но и тези, които поддържат и работят с компютрите.

Обрата връзка: Това е друг компонент от операционната система, който определя дали системата ще поддържа обратна връзка с потребителя като тази част не е задължителна.

1.2.Понятие за информационна система; основни термини и определения; етапи на развитие на информационните системи; съотношение между информационна система и информационна технология;

Всички свързани помежду си обекти представляват така наречената система. Тяхното поведение и характеристики се разглеждат като системни обекти. [1]

Система – това е едно цяло обръзувано от съвкупност от материални и нематериални обекти, обединени по някои общи признаци, предназначение, свойства, условия на съществуване, жизнен цикъл, функциониране и др.

Функциониране на система – процес на обработка на входно изходна информация имащ последователен характер във времето.

Подсистема – част от всяка система.

Свойства на системите в това число и на информационните системи:

Сложност – системата е зависима от множество влизащи в нея компоненти, от структорното им взаимодействие, а също така от сложността на вътрешните и външните връзки.

Делимост – системата се състои от ред подсистеми или елементи, разделени по определени признаци и отговарящи за конкретни цели и задачи.

Цялостност – означава всички елементи на системата да функционират като едно цяло.

Многообразие на елементите в системата и специфика на нейната природа – свойство свързано с функционирането на елементите, тяхната специфика и автономност.

Структорност – определя налично установените връзки и отношения между елементите вътре в системата, разпределението на елементите по нива и йерархично.

Адаптивност – приспособимост на системата в уславията на конкретна предметна област.

Интегриране – възможностите на системата да си взаимодейства с нови компоненти включващи се към нея или други подсистеми.

Всички системи значително се отличават една от друга, както по състав, така и по главните си цели. В последващата таблица 1 са представени няколко системи, състоящи се от различни елементи и направления за реализация на различни цели.

Система	Елементи на системата	Главна цел на системата
Фирма	Хора, обурудване, материали, сгради и др.	Производство на стоки и услуги
Компютър	Електронни и електромеханични елементи, връзки и др.	Обработка на данни
Телекомуникационна система	Компютри, модеми, кабели, програмно обезпечение и др.	Пренос на информация
Информационна система	Компютри, компютърни мрежи, хора, информационна и програмно обезпечение.	Производство на професионална информация

Таблица 1 Примери за информационни системи

Информационната система е взаимосвързана съвкупност от информационни, технически, програмни, математически, организационни, правови, ергономически, лингвистични, технологични и други средства, а също така персонал, която е предназначена да събира, обработва, запазва и подава икономическа информация, а също и да взема управленски решения. [4]

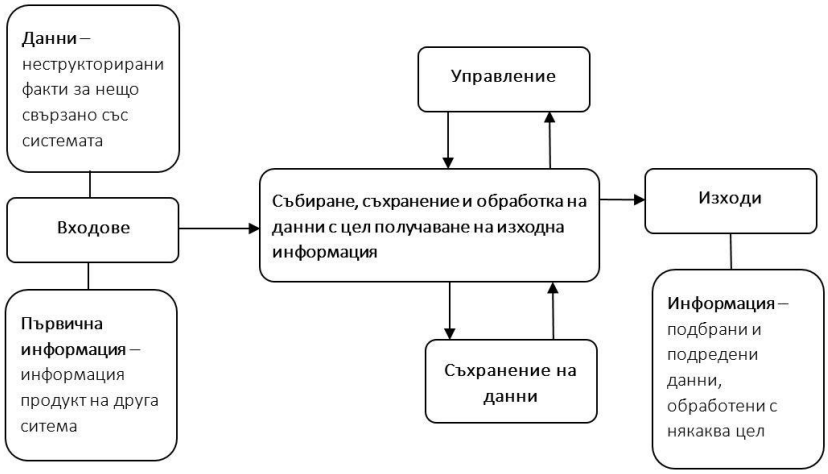
1.2.1.Свойства на информационните системи

Всяка информационна система може да бъде подложена на анализ, построена и управлявана на основата на общите принципи, на които се основават всички сложни системи. При изграждането на информационната система е необходимо да се използва системен подход. Информационната система представлява динамична и развиваща се система.

Информационната система следва да се разбира като система за обработка на информация идваща от компютърни и телекомуникационни устройства, реализирана на базата на съвременните технологии. Участието на човек в такава система се определя от нейната сложност, типа и набора от данни с които работи, както и от степента на офармяне на задачите нуждаещи се от разрешаване. [4]

1.2.2.Процеси в информационните системи

Въвеждане на информация от външни и вътрешни източници; Обработка на входящата информация; Записване на информацията за последващо използване; Извеждане на информацията в удобен за потребителя вид; Обратна връзка, тоест представяне на информацията след преработка в дадената организация за коригиране и оценка; [4]



Фиг. 02 Процеси в информационните системи

1.2.3.Икономическа информационна система (ИИС)

Представлява система чието функциониране във времето включва съхранение, обработка и разпространение на информация за дейности от икономическия свят. Информационните икономически системи са предназначени за решаване на задачи, обработка на данни, автоматизиране на офисни дейности, като се основават на метода на изкуствения интелект.

В зависимост от сферата на използване икономическите информационни системи се класифицират по следните видове:

- ✓ Икономически системи на фондовите борси;
- ✓ Застрахователни икономически системи;
- ✓ Статистически информационни системи;
- ✓ Икономически системи в данъчната сфера;
- ✓ Икономически системи в митническите дейности;
- ✓ Финансови икономически системи;
- ✓ Банкови икономически системи (БИС);
- ✓ Икономически системи на промишлени предприятия и организации (в това число влизат и счетоводните информационни системи);

1.2.4.Етапи на развитие на информационните системи

Първите информационни системи са се появили през 50-те години на 20 век. Първоначално те били предназначени за обработка на счетоводни документи и разчет на заплатите, а реалната дейност се осъществявала посредством електромеханични счетоводни сметачни машини. Това довело до намаление на разходите и времето за подготовка на необходимите хартиени документи.

60-те години се характеризират с изменение по отношение на информационните системи. Информацията получена от тях започнала да се използва периодично за отчетност по множество параметри. За изпълнението на това организациите се нуждаели от компютърно обурудване с широки възможности за използване, способно да обслужва множество функции, а не само да обработва счетоводни данни и да пресмята заплати.

През 70-те и началото на 80-те години, информационните системи започват да се използват масово в качеството си на средство за управление и контрол, поддържайки и ускорявайки процесите по взимане на решения.

В края на 80-те години концепцията по използването на информационните системи отново се изменя. Те се превръщат в стратегически източник на информация и се използват на всички нива в организациите от всякакъв тип. Информационните системи от този период се характеризират с това, че представят на време нужната информация, помагат на организацията да достигне нужния успех в своята дейност, създават нови продукти и услуги,

намират нови пазари, работят с точните за тях партньори, организират пускане на продукцията на много по ниска цена и множество други фактори.

1.2.5.Съпоставка между Информационна система и Информационна технология

Информационна технология – представлява процес от различни операции и действия върху обработваните данни. Всички процеси по преобразуването на информацията в информационната система се осъществяват с помоща на информационната технология.

Информационна система – среда от съставляващи елементи представляващи, компютри, компютърни мрежи, програмни продукти, бази данни, потребители, различни видове технически и програмни средства и др.

По този начин информационната технология се явява по широко понятие от информационната система. Реализацията на функциите на информационната система е невъзможна без знаията на оринтираната към нея информационна технология. Информационната технология може да съществува и извън сферата на информационната система. [4]

1.2.6.Състав и структура на информационните системи. Характеристики на функционални подситеми в информационната система

Структура – определена подредба на множество обекти и тяхната връзка, (фиг.03)

Фиг.03 Икономическа информационна система, състав

Функционална подсистема – подсистема реализираща една или няколко взаимосвързани функции.

Обезпечаваща подсистема – среда, в която се използват средства за преобразуване на информацията независимо от сферата на използване.

Функционалния признак определя назначението на подсистемата, а също така нейните основни задачи, цели и функции.

В ежедневната практика на производствените и търговски обекти с различни типове дейности, определящия функционален признак за класификация на информацинна система се явява:

Производствената дейност, свързана с непосредственото пускане на готовата продукция и насочена към създаване и внедряване в производството на научно-технически новости;

Кадрова дейност, насочена към подбор и направляване на необходимите за фирмата специалисти, а също така водене на служебна документация по различни аспекти;

Финансова дейност, свързана с организацията на контрола и анализа на финансовите ресурси на фирмата на основата на счетоводния, статистически и оперативен анализ и отчетност;

Маркетингова дейност включваща, анализи на пазара и продажбите, организиране на рекламни кампании свързани с представянето на продукцията и рационално организиране на материално-техническото снабдяване;

Основните направления и дейности на организацията определят и типа и вида на сбора от функционални подсистеми в информационната система. Най-общо могат да се разгледат следните видове:

- ✓ Производствени подсистеми;
- ✓ Кадрови подсистеми;
- ✓ Финансово счетоводни подсистеми;
- ✓ Маркетингови подсистеми;
- ✓ Допълнителни спомагателни подсистеми, изпълняващи функционални задачи в зависимост от спецификата на дейността на съответната фирма (например подсистема за ръководство на фирмата);

1.2.7.Характеристики осигуряващи подсистемите в информационната система

Програмно обезпечаване – съвкупност от програми осъществяващи функции и задачи в информационната система и обузпечаващи работата на компютърните технически средства. Инструктивно-методически материали по използването на средствата за програмно обезпечаване. Също така персонал, занимаващ се с разработката и обезпечаването на програмното обезпечаване през целия жизнен цикъл на информационната система.

Програмното обезпечение се разделя на:

- ✓ Ообщосистемно програмно обезпечение, което се класифицира според:
- ✓ Операционната система;
- ✓ Тестови и диатностични програми;
- ✓ Антивирусни програми;
- ✓ Командо-файлови процесори;

Операционните системи се явяват основните програмни комплекси изпълняващи следните основни функции:

Тестване работоспособността на изчислителните системи и съответните настройки при първоначалното включване;

Обезпечаване с апаратен, програмен и потребителски интерфейс;

Допълнителното програмно обезпечаване се касифицира така:

- ✓ Системи за подготовка на текстови документи;
- ✓ Системи за управление на бази данни;
- ✓ Системи за обработка на финасово-икономическа информация;
- ✓ Лични информационни системи;
- ✓ Системи за подготовка;
- ✓ Системи за управление на проекти;
- ✓ Експертни системи и информационни системи за поддръжка на вече приети решения;
- ✓ Системи за индивидуално проектиране и усавършенстване на управлението;

Техническо обезпечаване – представлява комплекс от технически средства, обезпечаващи работата на информационната система. Методически и ръководни материали, техническа документация и съответния персонал обслужващ тези технически средства.

В състава на комплексните технически средства обезпечаващи работата на информационната система влизат:

- ✓ Компютърни технически средства;
- ✓ Комуникационни технически средства;
- ✓ Организационно технически средства;

Компютърни технически средства – представляват базата от всички комплексни технически средства в информационните технологии предназначени за обработка и преобразуване на различни видове информация, която се използва в икономическата дейност.

Персонални компютри – изчислителни системи ресурсите на които са изцяло заети за обезпечаване работата на един служител (всички видове персонални компютри);

Корпоративни компютри – (main frame), изчислителни системи обезпечаващи съвместната дейност на множество служители в рамките на една организация, един проект или една сфера на информационна дейност с използването на едни и същи информационно изчислителни ресурси. Това са така наречените изчислителни системи с достъп на много потребители. Основно се използват в реализиране на по крупни проекти в областта на финансовите и производствените организации, при създаване на информационни системи обслужващи голям брой потребители в рамките на една определена функция (борсови и банкови системи, продажба на билети и др.).

Суперкомпютри – това са изчислителни системи използващи максимално достъпни и мощни изчислителни мощности и информационни ресурси. Основно се използват в военната, космическата област, а също и в областта на гробалните изследвания, прогнози и др.).

Комуникационни технически средства – те обезпечават една от основните функции на управленческата дейност, а именно предаването на информация в рамките на системното управление и обмена на данни с външна среда. Те предполагат използване на разнообразни методи и технологии, в това число и използване на компютърна техника. Към комуникационните технически средства се отнасят:

- ✓ Средствата и системите на стационарните и мобилни телефонни комуникации;
- ✓ Средствата и системите на телеграфните връзки;
- ✓ Средствата и системите на предаване на информация посредством факс и модеми;
- ✓ Средствата и системите на кабелната и радиовръзка, включваща и оптични кабелни връзки, а също и спътникови връзки;

Организационно техническите средства са предназначени за автоматизация и миханизация на управленската дейност. Съвкопността от организационно техническите средства може да се представи в следните групи:

- ✓ Носители на информация;
- ✓ Средства за създаване на текстови и таблични документи;
- ✓ Средства за копиране и размножаване на документи;
- ✓ Средства за обработка на документи;
- ✓ Средства за съхраняване, търсене и транспортиране на документи;
- ✓ Банкови организационно технически средства;
- ✓ Малогабаритна организационно техническа апаратура;
- ✓ Офисно обурудване;
- ✓ Допълнителни организационно технически средства;

Математическо обезпечаване – съвкупност от математически методи и модели и алгоритмична обработка на информацията използвана за разрешаването на икономически задачи в процеса на проектиране на информационните системи; техническа документация (описание на задачите, задание по алгоритмизация на икономико-матиматическите модели, задачи и конкретни примери за тяхното решение); персонал (специалисти по изчислителни методи, проектанти на информационни системи, доставчици на управленски задачи и др.);

Организационно обезпечаване – комплекс от документи регламентиращи дейността на персонала от информационната система в условията на нейното функциониране (връзки на работещите в управленските служби и обслужващия персонал на информационната система с използваните технически средства и помежду си). Организационното обезпечаване се изразява в методологии и ръководни материали в различните стадии на разработка, внедряване и експлоатация на информационната система.

Правно обезпечаване – съвкупност от правни норми, определящи създаването, юридическия статус и функционирането на информационната система, регламентиращи реда на получаване, преобразуване (обработка) и използване на икономическата информация

(закони, укази, постановления, заповеди, инструкции и други нормативни документи на министерства и ведомства, както и на местните органи на властта).

Ергономическо обезпечаване – представлява съвкупност от методи и средства използвани на различни етапи от разработването и функционирането на информационната система, предназначена за създаване на оптимални условия за висикоефективна дейност на човека (персонала) в тази система и нейното бързо усвояване. Към това се отнасят: коплекс от различни документи съдържащи ергономически изисквания към работните места, информационни модели, условия за действията на персонала, а също така и способи за реализация на тези изисквания и осъществевяване на ергономически експертизи по нивото на тяхната реализация.

Лингвистично обезпечаване – представлява съвкупност от езикови средства като език за управление и манипулиране на данните (системи за управление на бази данни); система от термини и определения използвъни в процесите на разработка и функциониране на информационната система; информационни езици за описание на структорната информация на информационната система (документи, показатели, реквизити и др.);

Информационно обезпечаване – представлява съвкупност от проектни решения за обема, разпределението, формата на представяне на информацията циркулираща в информационните потоци. То включва в себе си съвкупност от показатели, справочни данни, класификатори и кодиране на информацията, унифицирани системи за документиране, специализирана организация за обслужване, масиви от информация на съответстващите им носители, а също така персонал обезпечаващ надежното съхраняване, както и навременното и качествено обработване на технологичната информация;

1.3. Автоматизирани системи за управление – понятие и жизнен цикъл

Основната среда за приложение на информационните технологии в практиката са компютърните информационни системи. Те са тясно свързани с управлението и структурата както на съвременните фирми, така и на всички други дейности в обещественя живот. Чрез добро познаване на възможностите и тенденциите в развитието на компютърните информационни системи може да се повиши ефективността от работата на всички нива и във всички сфери на действие. Компютърните информационни системи са автоматизирани системи за управление, които се реализират на базата на съвременно високотехнологично хардуерно и софтуерно обурудване. [4]

За по-ясна представа свързана с автоматизираните системи за управление нека разгледаме следните основни понятия:

Информация – това са разнообразни познания и сведения за реалния свят, които се използват при взаимодействие с него. Основните характеристики на всяка информация са нейното съдържание (тоест смисъл, стойност на информацията) и ценност на информацията (тоест полезност, значимост). Информацията се получава в резултат на отражение на реалния свят, на различните обекти и процеси, протичащи в него. Всеки човек ежедневно получава информация навсякъде в средата, която го обкръжава.

Дейностите свързани с получаване на информация, съхраняване на информация, обработка на информация и разпространяване на информация се наричат информационни дейности, а всеки процес, който обхваща такива дейности – информационен процес.

Науката, която изучава начините за представяне на информацията, методите и средствата за автоматизиране на информационните дейности и процеси, като разглежда информацията като абстрактно понятие, независимо от рейлния обект или процес, чието отражение е тя се нарича информатика.

Основните направления в информатиката са: математическо осигуряване, програмиране, иконика, бюротика, изкуствен интелект.

В света на информатиката, информацията е измерима количествено:

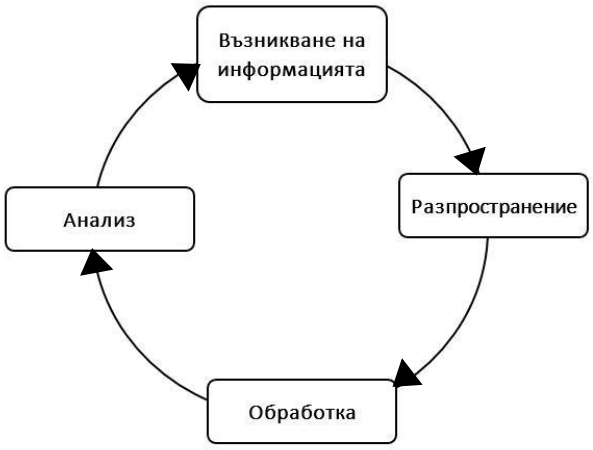
1 bit	Един бит е количестото информация за изхода от събитие, което има два равновероятности възможни изхода – 0 и 1
1 byte	Равен на 8 бита – основна мерна единица
1 KB	Равен на 1024 байта
1 MB	Равен на 1024 KB
1 GB	Равен на 1024 MB
и т.н.	

Таблица 2 Мерни единици за информация

В тясна връзка с понятието информация е и понятието съобщение. Това е понятие много близко до понятието информация, но има малко по-различно съдържание. Обикновенно съобщението се разглежда, като представено по определен начин информация. Съобщенията могат да се преобразуват по предварително замислени правила. Процесът на преобразуване на съобщения по някакви правила се нарича кодиране, а обратното преобразуване се нарича декодиране. Кодирането и декодирането се използват в информатиката като програмиране, което под една или друга форма е основен инструмент при създаването на компютърни информационни системи (или автоматизирани системи за управление). [3]

Едно от най-често използваните понятия в информатиката е понятието данни. Понятията информация и данни често пъти се възприемат като взаимозаменяеми, но това не е съвсем вярно. За целите на информационните системи, данните са различни факти регистрирани за различни събития, дейности и процеси в подходяща форма и върху определен информационен носител. Данните се въвеждат в информационните системи, за да се обработват и съхраняват с някаква цел. В този смисъл данните се разглеждат като вход в системата, тоест като суров материал, от който след обработка се получава информация. От такава гледна точка информацията се разглежда като данни, обработени по съответен начин, обикновенно с компютър. Във всички случаи на употреба, компютърната информационна система осъществява преобразуване на въведените данни в информация, която директно или индиректно се използва за управление.

Интересен е фактът, че информацията може да се разглежда от гледна точка на нейното възникване, разпространение, обработка и анализ.



Фиг. 04 Жизнен цикъл на информацията

Възникването на информацията, като първи етап от жизнения цикъл се отразява в информационната система чрез регистрирането на данни.

Обработката и анализа на данните или интерпретацията на знанията са базови функции на информационната система, които се получават чрез подходящо техническо и програмно осигуряване.

Изведените резултати носят информация, която спираловидно повтаря посочените етапи на жизнения цикъл.

Информационната система представлява съвкупност от дефинирани дейности, по въвеждане, обработка, съхранение и извеждане на информация, които се поддържат от нея. Във всички практически реализации на информационни системи, се извършва преобразуването на регистрираните занни в информация и това може да се счита за тяхна основна задача. Една информационна система се създава за осигуряване на субекта на управление с информация за оперативно, тактическо и стратегическо управление.

1.3.1.Основни типове автоматизирани системи за управление

Различават се два основни типа автоматизирани системи за управление:

а) Системи, които автоматизират технологични процеси, като управление на ракети, стругове, пещи и др., се наричат автоматизирани системи за управление на технологични процеси. Обекти за управление при тези системи са различни машини, уреди, устройства и др. В тях основна форма за предаване на информацията са различните видове сигнали (електрически, оптични, механични и др.), които постъпват в така наречените датчици. Автоматизираните системи за управление на технологични процеси са преди всичко автоматични системи за управление. Под автоматично система се разбира такава система, която може да функционира без участието на човека. Но при тях не винаги се прибягва до пълна автоматизация.

б) Системи, предназначени за автоматизация на процесите в икономическата и социалната сфера се наричат автоматизирани системи за организационно управление. Известни са още под названието управленски или мениджърски информационни системи. Обект за управление при тези системи са хората, човешките ресурси. В системите за организационно управление основна форма за предаване на информация са документите. Тези системи не могат да бъдат напълно автоматични, поради това, че човекът играе важна роля в управлението. Преди всичко той поставя и коригира целите и критериите за управление (те могат да се менят при изменение на условията). Освен това човекът внася творчески елемент при търсене на най-добрите пътища за постигане на поставените цели (например решително изменя технологията или организацията и др.). В управлението при окончателния избор на решение (от наличния многовариантен план на решения, които могат да бъдат приложени от автоматизираната система) и при предаване на юридическа сила на това решение от голямо значение е субективния фактор.

В последно време се наблюдава тенденция за сливане на двата типа системи в единни интегрирани системи за управление – комплексни Автоматизирани системи за управление или наричани още информационни системи. При това сливане все по голяма част от циркулиращатав системата информация се предава във вид на сигнали и специални типове документи на стандартни машинни носители (магнитни ленти, магнитни дискове, карти и др.). По този начин от гледна точка на формата за предаване на информация, границата между двата типа автоматизирани системи за управление се заличава да известна степен.

Функционално автоматизираните системи за управление могат да бъдат създавани в различни сфери и отрасли на техниката, икономиката, социалния живот. Но независимо от голямото разнообразие на функционалното предназначение на тези системи, по своята същност те имат обща информационна база на основата на процеса за автоматизираната обработка на информацията.

Системите, предназначени са събиране, съхраняване, обработване и търсене на информация, се наричат информационно-търсещи системи. Тези системи реализирани на базата на съвременната изчислителна техника се наричат автоматизирани информационно-търсещи системи. Те са ядрото на автоматизираните системи за управление. Формулирана е основната системно-техническа задача при проектирането на автоматичните системи за управление, като задача за оптимално формиране, рационална обработка и комплексно използване на информационните масиви в системата. Това води преди всичко към създаване

на големи интегрални бази от данни, които представляват информационната база на на мощните автоматизирани системи за управление.

Създаването на подобна база е един от най-трудните въпроси при разработката на автоматизирана система за управление. Именно масивите от данни, съхраняване и обработвани в една автоматизирана система за управление, обединяват в информационен план всички звена в системата.

Ефективното проектиране на структората на данните дава възможност оптимално да се построят подсистемите на паметта на информационно-търсещата част на системата, което ще позволи в голяма степен да се намали дублирането на данни, както и значително да се повиши ефективността при използване на информацията.

1.3.2.Данните – основен ресурс в информационните системи

Данните са основен ресурс в информационните системи. В средата на локална мрежа данните се ползват общо (shared) от потребителите. Разбира се запазват се и възможностите за еднопотребителска работа с тях. Тези данни, които са обявени за общо ползване (shared), са организиране и разпределени в бази данни. Последните могат да бъдат създадени от различни групи потребители по различно време или в процеса на проектиране на информационната система, базата данни да бъде разпределена така, че да допуска различните аспекти, релевантни към работата на отделните групи.

Поради необходимостта от осигуряване на коректни данни за всеки потребител на информационната система, без да се препятстват останалите, са създадени специални методи на достъп, а именно – конкурентен и неконкурентен. Когато данните се обработват от двама или повече потребители по едно и също време, се използва конкурентно поделяне на данни. Ако данните са поделени, но не се обработват в един и същи момент от различните потребители, поделянето е неконкурентно.

При информационни системи в средата на локална мрежа разпределението на ниво файл се извършва чрез монолитни файлове (не са структорирани в записи), като документи за обработка на текст, електронни таблици, публикации и графични изображения, които се разпределят между работната група. Разпределението на монолитните файлове се определя повече от адекватността на потребителските действия, отколкото от контролирането в програмите.

Информационните системи в средата на глобални мрежи използват частни (private) и обществени (public) бази данни. Частните се състоят от фирмени данни и външни данни, пряко използвани в процеса на обработка (пазарни показатели, стандарти, нормативи и др.). Обществените бази данни се поддържат в интернет. Техния брой и обеми непрекъснато се увеличава, а съдържанието им редовно се актуализира. Разходите за поддръжката им се осигуряват най-вече от фирмите, които са заинтересовани за рекламата.

Наличната информация в интернет е толкова много, че тя едва ил би могла да бъде включена в каталог или систематизирана. В допълнение към достъпа до повече от 1 милиард (2012) потребители притежаващи e-mail акаунти, всеки може да разглежда информацията и продуктите на десетки и стотици хиляди различни компании. Съществуват бази данни он-лайн съдържащи правителствена статистика, финансова информация, цени на акции, подробна информация за патенти, маркетингови източници, дистрибутори и др. За свободното време има бази данни с информация за филми, книги, клубове, къщи и коли, които се продават, наемат и др. Съществуват и групи за новини – (newsgroups), представляващи форуми за дискусии и те са едни от най-активните части на интернет. Също така следва да се спомет и така наречените социални мрежи и сайтове, предлагащи разнообразни услуги и информация за собствените си потребители, както и даващи възможност за директни социални контакти в мрежата. [5]

Накратко в интернет може да се узнае какво е времето в коя да е част на света, да се проследят последните световни новини, да се следат цените на акциите, да се проучват бъдещи клиенти, да се проверяват кредитни статуси, интернет банкиране и множество други дийности.

Извличането на информация от обществените бази данни може да стане чрез директно свързване на определен адрес (URL – Universal Resource Location) или като се използват така наречените машини за търсене. Те представляват специални програми тип паяци, които претърсват уеб пространството за нови и вече съществуващи страници с информация. Те съобщават срещаните думи и съответните адреси на страниците на програмите за търсене.

Огромния обем на данни изисква изключително точна и надеждна работа, защото при грешка, последиците могат да бъдат непредвидими.

Консултанти и компании, занимаващи се с проблемите за сигурността на фирмените данни и информацията в интернет, твърдят, че един от най-добрите начини да бъде защитена една компания срещу атаки е да се използва така наречената огнена стена (firewall). За съжаление далеч не всички разбират нейното значение и функции.

Огнената стена представлява специално софтуерно приложение, което преглежда цялата информация прехвърляна от и към интернет. Този софтуер може да се конфигурира така, че да търси определен вид информация, например команди, които не трябва да се изпълняват на интернет сървъри, или да блокира информацията идваща от определен потребител. Работата на огнената стена и да блокира подобни неоторизирани команди, без да пречи на работата на добронамерените потребители. Това обаче е нелека задача, тъй като хакерските техники и методи непрекъснато се усавършенстват, както и самите технологии и изпозвани софтуери.

Повечето от съвременните софтуерни продукти за сървъри включват характеристики, които позволяват конфигуриране на сървъра така, че да бъдат блокирани голям кръг от техники използвани за проникване отвън.

Основните правила за контрол на данните в информационните системи са така наречените EDP-контроли и засягат петте компонента на информационната система – хардуер, софтуер, инструкции, данни и персонал. Те редуцират неоторизираните действия, компютърните престъпления и случайните загуби. За утвърждаване значението на информационната система за фирмата преодоляване на опитите за компютърни престъпления се изисква мениджърите да показват категорично, че я признават за полезна и интегрална част от бизнеса. С поведението си те трябва да показват, че съвременната информационна система не само поддържа бизнеса, а че тя е бизнеса.

Мениджърите трябва да управляват такава система, както правят това за другите дейности и да обръщат внимание на възникналите проблеми. Те трябва да изискват периодични отчети за работата на системата като:

- ✓ Брой обработени транзакции;
- ✓ Процент време, през което тя е била достъпна или не;
- ✓ Часове безпогрешна работа и др;

Мениджърите могат да проучват дали потребителите са удовлетворени от информационната система и да се интересуват от изискванията и препоръките им.

В страните с практика на използване на информационните системи в средата на глобална мрежа, центровете за фирмени данни са разположени на изолирани места. Достъпът до центъра е строго контролиран. Процедурите за контрол са старателно планирани и контролирани.

Наблюдаваните тенденции към глобализация на бизнеса ще доведат до утвърждаването на информационните системи в глобални мрежи.

1.3.3.Жизнен цикъл на автоматизираните информационни системи; Модел на жизнен цикъл на автоматизирана информационна система

Жизнен цикъл на информационната система представлява периода на създаване и използване на информационната система, започвайки с момента на възникване на потребността от нея и завършвайки с момента на пълното и извеждане от експлоатация. [3]

Стадии на жизнения цикъл на информационната система:

Предпроектно изследване – сбор на материали за проектиране, като се обръща внимание на предварително зададените параметри и нужди, изучаване обекта на автоматизиране, издаване на предварителни изводи и проектни варианти на информационната система;

Проектиране:

Предварително проектиране – избор на проектни решения свързани с аспекти по разработката на информационната система; описание на реалните компоненти на информационната система; оформление и утвърждаване на техническия проект;

Детайло проектиране – избор или разработка на математически методи и алгоритми; корекция на структурите; създаване документация за доставка, инсталиране на програмните продукти; избор на комплекс от технически средства и документация за тяхното инсталиране;

Разработка на технически работещ проект на информационна система;

Разработка на методология за реализиране на функциите за управление с помощта на информационната система и описание на регламента от действия на апаратното управление;

Разработка на информационната система – доставка и инсталиране на техническите и програмни средства; тест и настройки на програмния коплекс; разработка на инструкция за експлоатация на програмно-техническите средства;

Пускане на информационната система в действие – активиране на техническите средства; активиране на програмните системи; обучение и сертифициране на персонала; тестов цикъл; предаване на системата и подписване на приемо-предавателен протокол;

Работа на информационната система – ежедневна експлоатация; съпровождащи дейности от ежедневната работа;

Модели на жизнения цикъл на информационните системи:

Каскаден модел – осъществява се преход към следващия етап след пълно приключване на работата по предходния етап. Модела демонстрира класически подход в различни области на приложение.

Повтарящ модел – поетапен модел с вмъкнати междинни етапи за контрол и обратна връзка. Преимуществото на този модел е във възможността за поетапно коригиране, което обезпечават по лека работа в сравнине с каскадния модел. В същото време живота на всеки етап е разчетен на живота на целия период на разработка.

Спирален модел – този модел се характеризира със спиране в началните етапи на анализ и проектиране. Този модел представлява непрекъснато повтарящ се модел на разработка, където всеки етап (цикъл), представлява сам по себе си завършен цикъл на разработка, водещ до пускане на изделието в действие (версия на проекта на информационната система), което се усавършенство след всяка нова разработка, за да се получи значима информационна система. По този начин всяка витка на спиралата съответства на етап от модела на създаване на информационната система, тоест има непрексъната задълбочаване и последователно конкретизиране на окончателния вариант на информационната система, който да доведе впоследствие до нейната реализация.

1.4. Класификация на информационните системи; Типове информационни системи

Информационните системи могат да се класифицират най-общо по три критерия:

- ✓ Тип на информационната система;
- ✓ Класификация по функционални признаци;
- ✓ Класификация по ниво на управление;

Фактографически и документални информационни системи

Типа информационна система зависи от това чии интереси обслужва тя и на какво управленско ниво функционира. По характера на представянето си и логическата организация

на съхраняваната информация, информационните системи за разделят на фактографически, документални и геоинформационни.

Фактографически информационни системи

Те събират и съхраняват данните във вид на множество екземпляри от един или няколко типа структорни елементи (информационни обекти). Всеки един от тези екземпляри или съвкупност от тях, отразява сведения свързани с някакъв факт или събитие отделно от всички останали сведения и факти.

Структурата на всеки тип информационен обект се състои от окончателен набор от реквизити отразяващи основните аспекти и характеристики на обекта от съответната област на използване. Окомплектоването на информационна база в фактографическа информационна система включва включва, като правило, задължителен процес на структоризация на входната информация.

Фактографическите информационни системи предполагат удовлетворяване на информационните потребности непосредствено, тоест представяне на сведенията на самия потребител (данни, факти, концепции).

В документалните (документираните) информационни системи единичен елемент на информация се явява неразделения на малки части документ и информацията при входа (входен документ), по правило тя не се структорира или ако се струторира, то в съвсем ограничн вид. За входния документ могат да бъдат установени някои формални позиции (дата на създаване, изпълнител, тематика).

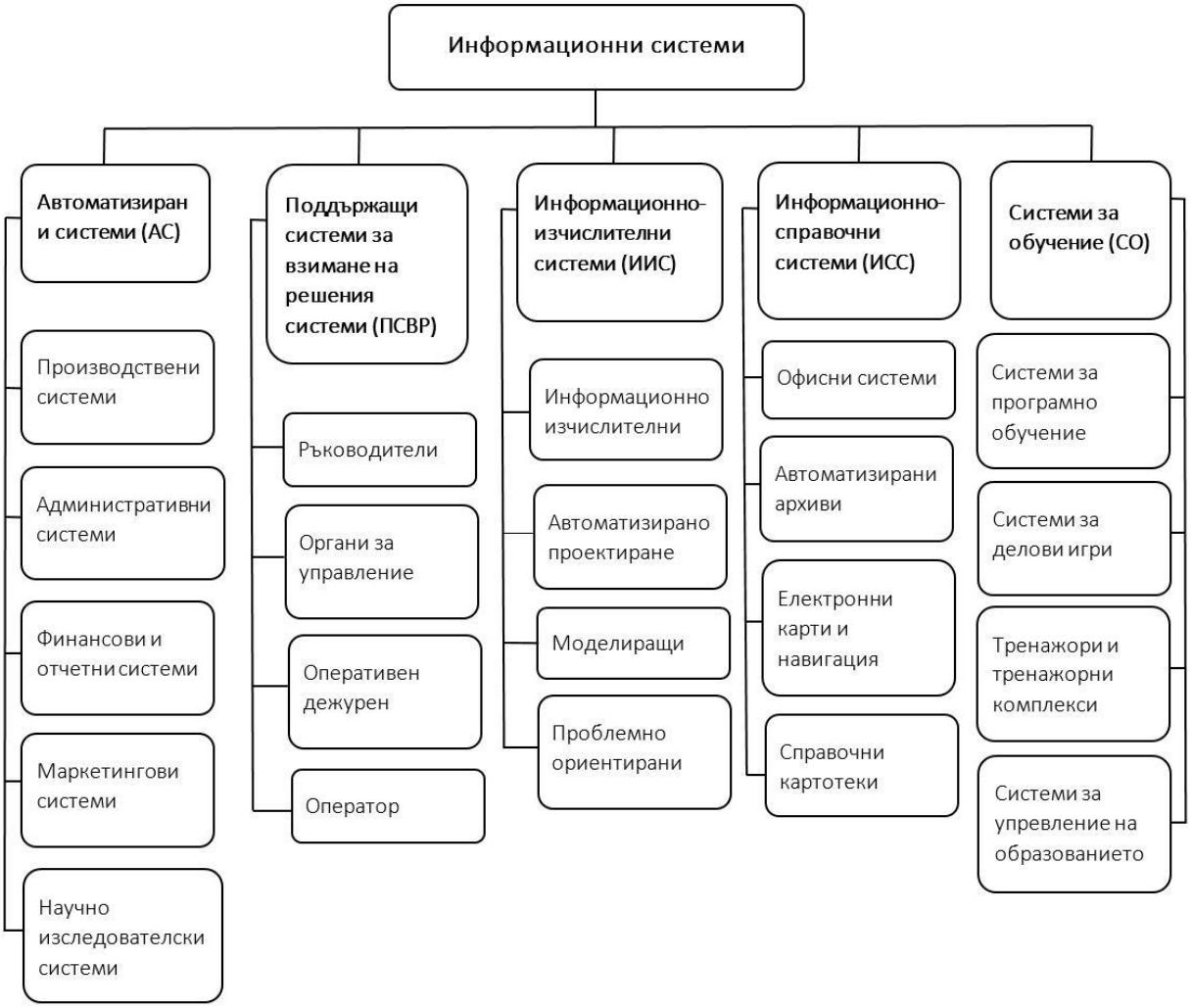
Някои видове документални информационни системи обезпечават установяването на логическа връзка между входящите документи – съподчиненост по смисъла на съдържанието, взаимни препратки по различни видове критерии и др.

Определянето и създаването на такива взаимовръзки, само по себе си представлява сложна, многокритерийна и мултиаспектна аналитическа задача, която не може да се формализира напълно.

В геоинформационните системи данните са организирани във вид на отделни информационни обекти (с определен набор от реквизити), свързани към обща електронна топографическа основа (електронна карта). Геоинформационните системи се използват за информационно обезпечаване в тези области структората и информационните обекти в които съдържа пространствено географски компонент (транспортни машрути, комунални комуникации и др.).

1.4.1.Класификация на информационните ситеми по функционални признаци

Функционалния признак определя предназначението на подсистемите а също така нейните основни цели, задачи и функции. На фиг. 05 е представена класификацията на информационните системи по характеристики на техните функционални подсистеми.



Фиг. 05 Класификация на информационните системи по функционални признаци

В икономическата практика, производствените и търговски обекти, вида дейност на които се определя по функционални признаци на класификация на информационната система, влизат производствени, маркетингови, финансови, кадрови и др. дейности.

1.4.2.Класификация на информационните системи според нивото на управление

Основно се разделят на:

- ✓ Информационни системи на оперативно ниво – счетоводни, банкови депозити, обработка на поръчки, регистрация на билети, изплащане на заплати;
- ✓ Информационна система за специалисти – офисна автоматизация, обработка на данни (включително експертни системи);
- ✓ Информационна система на тактическо ниво (средно звено) – мониторинг, администриране, контрол, взимане на решения;
- ✓ Стратегически информационни системи – формулиране на цели, стратегическо планиране;

- ***Информационни системи на оперативно ниво***

Тези системи обезпечават работата на специалисти изпълнители, обработвайки данни за транзакции и/или събития (отчети, сметки, заплати, кредити, потоци от суровини и материали). Предназначението на информационната система на това ниво е да отговаря на търсенията за текущото състояние и да проследява потока от сделки в съответната фирма, което е равносилно на оперативно управление. За да се справи с тези задачи, информационната система трябва да бъде леснодостъпна с непрекъснато действие и да представя точната информация.

Задачите, целите и източниците на информация на оперативно ниво са предварително определени и в значителна степен структорирани. Решението е запрограмирано в съответствие със зададените алгоритми.

Информационната система на оперативно ниво се явява свързващо звено между фирмите и външната среда. Ако системата работи недобре, то организацията или не получава външна информация, или не предава такава навън. Освен това тази система е основният доставчик на информация за останалите типове информационни системи в организацията, в този смисъл тя съдържа както оперативна така и архивна информация.

- ***Информационни системи за специалисти***

Информационните системи на това ниво подпомагат специалистите, работещи с данни, повишават продуктивността и производителността на инженерната работа и проектантите. Задачата на подобни информационни системи е да интегрират новите сведения в организацията и да окажат помощ в обработката на различните видове документация. По примера как индустриалното общество все повече се трансформира в информационно, производителността на икономиката все повече и повече зависи от нивото на развитие на тези системи. Подобни системи във вид на работни станции и офисни системи са едни от най-бързо развиващите се в съвременния бизнес.

- ***Информационна система за офисна автоматизация,*** вследствие на своята простота и многопрофилност активно се използва от работниците на всякакво ниво в организацията. Най-често се използват от работници от средно ниво: счетоводители, секретарки, чиновници. Основната им цел е обработка на данни, повишаване ефективността на работата и опростяване на канцеларския труд. Информационните системи за офисна автоматизация свързват в едно цяло работниците в информационната сфера от различни региони и спомагат за поддържане на връзка с клиентите, доставчиците, както и с други организации. Тяхната дейност основно обхваща управлението на документацията, комуникациите, съставяне на разписания и др.

Тези системи изпълняват следните функции:

- ✓ Обратка на текстове с компютър с помоща на съответното програмно обезпечение;
- ✓ Производство на висококачествена печатна продукция;
- ✓ Архивиране на документи;
- ✓ Електронни календари и работни книжки за водене на деловодство;
- ✓ Електронна и стандартна поща;
- ✓ Видео и телеконференции;

- ***Информационните ситеми за обработка на знание***, в това число и експертните системи събират в себе си знанията, необходими на инженерите, юристите и учените при разработка или създаване на нов продукт. Тяхната работа се заключава в създаването на нова информация и нова инженерно и научно проектиране, което позволя да се обезпечи високо ниво на техническите разработки.

1.4.3.Информационни системи на тактическо ниво (средно звено)

Основните функции на тези онформационни системи са:

- ✓ Сравнение на текущите показатели с минали такива;
- ✓ Съставяне на периодични отчети за определено време (а не издаване на отчети за текищи събития, както е на оперативно ниво);
- ✓ Обезпечаване достъпа до архивна информация и др.;

1.4.4.Система за поддръжка при вземане на решения. Те обслужват частично структорирани задачи, резултатите от които е трудно да бъдат прогнозирани предварително (имат по-мощен аналитичен апарат с няколко вида модели). Те получават информация от управленските и операционните информационни системи. Този вид системи се използват от

всички, чиято работа е вземането на решения: мениджъри, специалисти, аналитици. Например по тяхна препоръка може да се вземе решение за покупка или наемане на ново обурудване.

Тези системи имат следните характеристики:

- ✓ Обезпечават решението на проблеми, чието развитие е трудно да бъде прогнозирано;
- ✓ Снабдени са със сложни инструментални средства за моделиране и анализ;
- ✓ Позволяват лесна смяна на постановката на решаваните задачи и входните данни;
- ✓ Отличават се с гъвкавост и лесно се адаптират към измененията на условията, дори по няколко пъти на ден;
- ✓ Притежават технология максимално ориентирана към ползвателя;

1.4.5.Стратегически информационни системи

Развитието и успеха на всяка организация или фирма основно се определя от избраната от нея стратегия. Под стратегия тук се разбира набора от методи и средства за решение на перспективни и дългосрочни задачи. В този контекст може да се използват и понятията, стратегически метод, стратегическо средство, стратегическа система. В съвременния свят във време на преходи към нови и различни пазарни отношения въпросите за стратегията, развитието и поведението на фирмата са изключително важни и на тях следва да се обръща значително внимание. Това от своя стряна води до сериозно изменение на това как се възприемат и използват информационните системи. Те все повече се възприемат като стратегически важни системи, които оказват влияние на избора на цели фирми, техните задачи, методи, продукти, услуги, позволяват да се изпревари конкуренцията, а също така позволяват по-тясна взаимовръзка на потребителите с достачците на стоки и услуги. Така се появява нов тип информационна система – стратегическата.

Стратегическата информационно система представлява компютърна информационна система, обезпечаваща поддръжката по вземане на решения и реализацията на перспективни стратегически цели в развитието на организацията. Съществуват ситуации при, които качеството на информационната система, води до изменение не само на структурата, но и целия профил на съответната фирма или организация, което от своя страна води до нейното по-добро развитие. Но в същото време е възможно и възникването на нежелателни психологически проблеми, свързани с автоматизацията на някои функции и видове дейност, тъй като това може да постави част от работещия в тази област персонал в неизгодно положение, или изцяло да замени нуждата от такъв.

1.5. Допълнителна класификация на информационните системи

1.5.1.Класификация според степента на автоматизация

В зависимост от степента на автоматизация на информационните процеси в системата на управление на фирмата, информационните системи се определят като ръчни, автоматични и автоматизирани.

- ***Ръчните информационни системи*** се характеризират с отсъствието на съвременни технически средства за обработка на информацията, а всички опирации се изпълняват от персонала. Като пример може да се вземе дейността на мениджър в фирма, където липсват компютри. В този случай може да се каже, че той работи с ръчни информационни системи.
- ***Автоматичните информационни системи*** изпълняват всички операции по обработката на информацията без участието на човек.
- ***Автоматизираните информационни системи*** предполагат участие на персонал в процеса по обработка на информацията, както и на технически средства, като главната рола се изпълнява от компютрите. В съвременните тълкувания в термина „информационна система“, задължително се включва и понятието автоматизирана система. Автоматизираните информационни системи, имайки се предвид широкото им използване в

организацията на процесите на управление, имат различни модификации и могат да бъдат класифицирани, например по характера на обработваната информация и по сферата на използването и.

Пример: Ролята на счетоводителя в информационната система за изчисляване на работната заплата се заключава в задаване на изходни данни. Информационната система ги обработва по предварително зададени алгоритми с подаване на резултатите във вид на ведомости отпечатани на хартиен носител.

1.5.2.Класификация според характера на използваната информация

- ***Информационно-търсещи*** – те обезпачават вкарването, систематизирането, съхранението и подаването на информация при поискване от ползвателя, без сложни преобразувания на данните. Пример за такива системи са информационно-търсещите системи в библиотеките, разписания в различните видове транспорт и др.).
- ***Информационно-решаващи*** – тези системи осъществяват всички операции по обработката на информацията по определени алгоритми. Сред тях може да се направи класификация по степеннта на въздействие на изходния резултат на обработената информация в процеса на вземане на решение – управляващи и съветващи системи.

Управляващите информационни системи изработват информация на основата на която човек взима решения. За тези системи са характерни задачи за пресмятане и обработка на по големи обеми от данни. За пример може да се даде система за оперативно планиране на продукция и система за счетоводно отчитане.

Съветващите информационни системи изработват информация, която се прима под формата на сведения от ползвателите и не се превръща непременно в серия от определени действия. Тези системи претежават по висока стипен на интелект, тъй като за тях е характерна обработката на знание, а не само на данни. За пример може да послужи медицинска информационна система за поставяне на диагноза на пациент и предписване на предполагаема процедура на лечение. Лекарят може да приеме получената информация като сведение, но също така да предложи и друго решение в сравнение с предложеното от системата.

1.5.3.Класификация според сферата на използване

- ***Информационни системи за организационно управление***, които са предназначени за автоматизиране функциите на управленския персонал. Като се има предвид широкото използване и разнообразие на този клас системи, често за всеки тип информационна система се има предвид информационната система за организационно управление. Към този вид системи спадат както информационните системи за управление на промишлени предприятия, така и такива за непромишлени обекти: заведения, банки, търговски фирми и др.
- ***Информационните системи за управление на технологични процеси*** служат за автоматизиране на функциите на производствения персонал. Те широко се използват при организация на поточни линии, изработка на микросхеми, сглобка на детайли, за поддръжка на технологичния процес в металургическите и машиностроителни промишлени предприятия.
- ***Информационните системи за автоматизирано проектиране*** са предназначени за автоматизиране на функциите на инженерите проектанти, конструктори, архитекти и дизайнери при създаването на нови техники и технологии. Основните функции на подобни системи се явяват: инженерни пресмятания, създаване на графична документация (чертежи, схеми, планове), създаване на проектна документация, моделиране на обекти за проектиране.
- ***Интегрираните (корпоративни) информационни системи*** се използват за автоматизация на всички функции във фирмата и обхващат целия цикъл на работа, от проектирането до готовата продукция. Създаването на такива системи е сравнително трудно, тъй като изисква системен подход изхождайки се от главната цел, например получаване на печалба, завюване на нови пазари и др. Такъв подход може да доведе до изменение на

цялостната структора на фирмата, а това е стъпка, която далеч не всеки ръководител би предприел.

Глава 2. ФИНАНСОВИ ИНСТИТУЦИИ

Във финансовата икономика финансова иституция е институция, която осигурява финансови услуги за своите клиенти или членове. Може би най-съществената финансова услуга, предлагана от финансовите институции е работата като финансови посредници. Повечето финансови институции са регулирани от правителството. [5]

В по-широк смисъл финансовите институции могат да се разделят на:

- Взимащи депозити институции, които вземат и управляват депозити и дават заеми, като банки и други;
- Застрахователни компании и пенсионни фондове;
- Брокери, инвестиционни фондове и др;

Финансовите институции се делят също на банкови, небанкови и други.

- ***Банкови финансови институции***

Тук спадат универсалните и инвестиционните банки.

- ***Небанкови финансови институции***

Представени са от застрахователните дружества (ЗД), пенсионните фондове (ПФ), здравните фондове, инвестиционните дружества и колективните инвестиционни схеми (КИС).

- ***Други финансови институции***

Факторинговите и форфетинговите дружества.

2.1.Банкови финансови институции

Главният фактор, по който банките се различават е възприетата организационна структура, която е специфична за всяка отделна банка. Затова не може да се говори за общоприета или типична такава. Това, което определя организационната структура на банката е нейната стратегия. Организационната структура е основата в чиито рамки институцията функционира. Тя обхваща подредените по определен йерархичен ред основни звена в кредитната институция. [8]

Организационната структура в банката се прави така, че ръководството да може да изпълни две важни задачи: специализация и координация на дейностите. Ако организационната структура е правилно разработена, банката би следвало да извлече главната полза от специализацията – т.нар. икономия от мащаба, а от координацията – икономия от обхвата.

Банковата система представлява съвкупност от банките на страната в тяхната взаимна обвързаност, подчиненост и законова регламентация. Съвкупността включва всички банки или лицензирани банкоподобни институции, които извършват банкова дейност, определена в съответните законови и нормативни документи на страната. Лицензът се дава след като се прецени характерът на дейността, възможностите за извършване на тази дейност, наличието на необходимея капитал, квалификацията на тази дейност, наличието на необходимия капитал, квалификацията на управляващите органи и други изисквания, гарантиращи нормална банкова дейност.

Съществуват три групи банки:

Емисионни (централни) банки, основната дейност на които е свързана с емисионни операции-издаване на банкноти, книжни пари, ценни книжа. [6]

Търговски банки - гръбнака на финансовата система, чиято стабилност е едно от най-важните условия за функционирането на пазарните механизми, за ръста на националната икономика, за благосъстоянието на гражданите. [6]

Банкоподобни институции - Банкоподобните (Небанковите) финансови институции са лицензирани финансови и инвестиционни компании, дружества за електронни пари, брокери на ценни книжа, лизингови дружества и др. Основни области на специализация на банкоподобните институции са операции на паричния пазар, операции на капиталовия пазар, финансиране, инвестиране, проектиране, консултиране, проучване и анализиране, електронна търговия, финансово управление, инвестиционно посредничество и банкиране. [6]

Банковата система се характеризира от взаимоотношенията между централната банка и търговските банки. От значение е и структурата на самите търговски банки и лицензираните небанкови институции. Връзките и зависимостите между структурните звена се определят от съответните закони. Прилагат се и традиционните правила и обичаи в банковото дело в условията на пазарната икономика.

В зависимост от мястото на емисионната банка в системата от банки, банковата система се определя като:

- ✓ Еднозвенна;
- ✓ Двузвенна;

При еднозвенната банкова система емисионната банка има функции и на обикновена търговска банка. В този случай тя обслужва държавата и всички останали икономически субекти в страната: лица, предприятия, учреждения. Наред с това тя има и задачата да обслужва държавата и паричното обръщение-чрез емисията на парите, контрола върху парите и паричното обръщение.

При двузвенната банкова система емисионната банка се отделя от редицата на останалите търговски банки се издига над тях като банка на банките, нейни клиенти са държавата и търговските банки. Този вид система повишава значително възможностите за регулиране на самата банкова система чрез икономически лостове на централната банка върху търговските банки и чрез съответните законови и правни регламентации. Разкриват се и по-големи възможности за провеждане на държавната политика в областта на паричното обръщение и кредита, за защита на интересите на вложителите и за поддържане стабилността на паричната единица. Разкриват се по-големи възможности за регулиране ликвидността на банките и за спазване изискванията за капиталова адекватност на банките.

За начало на банковата система в България се приема създаването на Българската Народна Банка (1879), непосредствено след Освобождението. [8]

Тя е учредена като обикновена търговска банка, която има за задача да обслужва и държавата. По-късно се правят опити за нейното превръщане в банка на банките - реално това се постига при създаването на двузвенната банкова система у нас и прехода към пазарна икономика.

В периода от 1951г. - 1987г. банковата система на България е еднозвенна. Емисионната банка изпълнява и функциите на обикновена търговска банка.

Началото на прехода към двузвенна банкова система у нас бе поставено през 1987г. Тогава се създават специализирани отраслови търговски банки за дългосрочно кредитиране само на съответните отрасли.

Истинска класическа двузвенна банкова система у нас се въвежда през 1991г. с въвеждането на валутния борд. През периода на финансовата стабилизация на страната,

банковата ни система се характеризира от промените в самата централна банка, намаления брой на функциониращи търговски банки, приватизирането на банките и навлизането на чуждестранни банки в страната.

Схема за съвременната ни банкова система:

Фиг. 06 Съвременна банкова система

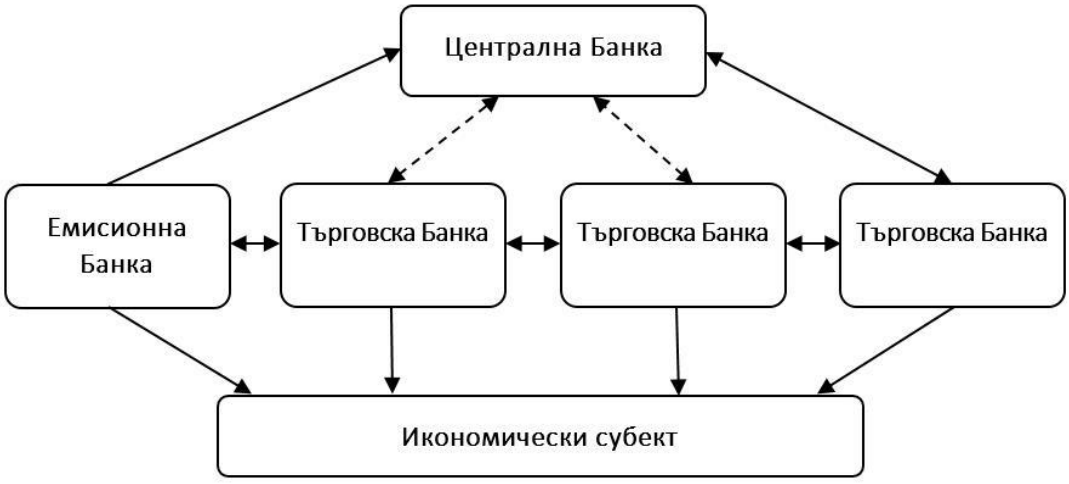
Централните банки възникват по два начина:

- ✓ Еволюционен;
- ✓ Законодателен;

Еволюционен е този начин за възникване на централните банки, при който вече съществуващата търговска банка се превръща в емисионна.

При *законодателния* начин още със създаването на централната банка със законодателен акт тя се определя като единствената емисионна банка - банка на банките и банка на държавата.

Преобладаващ е еволюционният път за възникване. Банката се отделя от другите банки, развивайки специфичната си дейност по емисията на банкноти. С развитието на стоково-паричните отношения нейната функция все повече се разграничава от дейността на останалите търговски банки. Така централната банка се обособява като емисионна, която има за клиенти другите търговски банки и държавата. Емисионната банка се превръща в централна, т. е. в банка на банките.



Фиг. 07 Превръщане на емисионната банка в централна банка

Обособяването на централните банки в различните страни става в различни исторически периоди. Приема се, че първата централна банка в света е Шведската държавна банка, основана през 1668г.

В Англия със специален закон от 1694г. се образува Английската банка като емисионен институт с частен акционерен капитал. Основната цел на Bank England при нейното създаване е била да финансира разходите на правителството във връзка с войната с Холандия. От 1844г. тя поема функциите на централна емисионна банка и банка на банките. През 1946г. е национализирана. Най-характерно за структурата на Английската банка са двата основни департамента-емисионен и банков.

- емисионният департамент ръководи емисията на пари, следи за концентрирането на свободните парични средства на останалите банки, регулира кредитния и паричния пазар.
- банковият департамент извършва операции по концентриране на депозитите от банките, правителството, за покупка на ценни книжа от паричния пазар.

След Втората световна война на територията на Федералната република и Западен Берлин, на мястото на напълно обезценената райхсмарка се въвежда германската марка и се предприема изграждане на двустепенна централизирана банкова система с федеративна структура. Така Deutsche Bundesbank става приемник на създадената през 1876г. Дойче Райсбанк като централна банка на Германия. Тя е едновременно гарант на националната валута, емисионен институт, банка на банките и банка на държавата.

Във Франция централната емисионна банка е създадена като частно акционерно дружество през 1800г. Тя е имала като главна задача да издава банкноти, платими на преносител, да мобилизира свободните парични средства, да сконтира менителници. Придобива постепенно монопол на парична емисия към средата на XIX в., изземвайки тези права от някои банки в различните департаменти.

Ролята на централната банка в САЩ изпълнява създадената през 1913г. Федерална резервна система, състояща се от Съвет на управляващите, 12 федерални резервни банки, Федерален консултативен съвет.

Централните банки започват да се оформят към началото на XX в. Тогава за тях стават типични функциите на емисионен институт, банка на банките, банка на държавата и съхранение и управление на златно-валутните резерви на страната. През периода на възникване заедно с функцията еволюира и формата на собственост и на централните банки. Докато първоначално преобладава частно-правната форма на собственост и организация на емисионните банки. Първата световна война започва процес към одържавяване на централните емисионни банки.

Една от основните характеристики, която дава облика на централната банка, е обстоятелството, че тя обслужва държавата:

- ✓ съхранява златно-валутните резерви на страната;
- ✓ води сметките на държавата;
- ✓ изпълнява касово бюджета на страната;
- ✓ провежда парично-кредитната политика;

По тези характеристики централната банка се определя като банка на държавата, независимо от характера на нейната собственост подчиненост. В много случаи централната банка юридически е независима от правителството на страната и се отчита само пред парламента, който избира нейното ръководство и приема отчетите за дейността й. Това е характерно за централните банки в страните с развита пазарна икономика.

Класически се наричат тези функции на централната банка , които разкриват нейната основна характеристика и същевременно я отличават от търговските банки и другите субекти на банковата система. Това са:

- ✓ емисионна функция;
- ✓ регулираща функция;
- ✓ функция контрол и надзор върху банковата система.

Емисионната функция е определяща за централната банка. Тя емитира в обръщение парите под фармата на банкноти и монети. Тя е институция, която е натоварена да поддържа баланс между парите в обръщение и стоките, подлежащи на реализация.

Регулиращата функция се изразява във въздействието върху паричните процеси и оттам върху икономическите процеси в страната. За тази цел централната банка използва паричните инструменти, с които разполага и в съответствие със законните й пълномощия. Чрез увеличаване или намаляване на паричната маса централната банка въздейства на паричното предлагане и на стопанската активност.

Третата функция на централната банка е *контрол и надзор* върху търговските банки и останалите лицензирани финансови институции. Чрез контрола централната банка гарантира платежноспособността на банките, не допуска системен риск, защитава вложителите, създава условия за нармална конкуренция между банките. Централната банка осъществява надзор върху банките в два аспекта:

- ✓ институционален;
- ✓ функционален;

Институционалният надзор от централната банка се изразява в издаването на лицензи на новосъздавани банки и на лицензи при преструктуриране в процеса на дейността им. Стремежът е създаването на нови банки да е икономически обосновано и да има свободно поле за дейност в банковата система на страната.

Функционалният надзор на централната банка включва надзора на вече лицензираните и функциониращи търговски банки, като следи за финансовата стабилност на банките, изпълнението на показателите за ликвидност, степента на риск, капиталовата ликвидност, степента на риск, капиталовата адекватност.

Централната банка може да налага санкции на търговските банки за канстатирани нарушения, за неефективна банкова дейност, за нарушаване на изискванията и показателите за тази дейност, да предприема мерки за оздравяване на банките. При положение, че мерките на централната банка не премахнат опасността от неплатежноспособност на съответната банка, тогава централната банка може да предприеме откриване на производство по несъстоятелност на изпадналата в криза банка.

Парично-кредитните механизми и инструменти за регулиране на икономиката от централната банка са:

А) ***Парична емисия*** понятието включва пускането от емисионата банка на нови, допълнителни количества монети и банкноти, с което се увеличава паричната маса в обръщение. В исторически план понятието емисия се развива от пълноценното парично обръщние до обръщението в съвременните условия. При банкнотното обръщение емисията на банкноти е зависела не само от съответните запаси от благороден метал в централната емисионна банка, а и от кредитното обезпечение, покрито с полиците.

Основен емисионен институт е централната емисионна банка. Търговско-депозитните банки също могат да пускат платежни средства чрез кредитиране на икономически агенти и покупка на съкровищни бонове, които превръщат дълга на бюджета в платежни средства.

Съвременната парична емисия може да се разглежда като:

- ✓ класическа парична емисия, която се осъществява от централната емисионна банка;
- ✓ депозитно-кредитна парична емисия, основана на депозитно-кредитните операции на търговските банки.

В) ***Сконтова политика*** - един от най-старите инструменти на централните банки за осъществяване на парично-кредитна политика от XIX век.

Същността на сконтовата политика се състои във въздействието върху сконтовите кредити и паричната база. Това става чрез промяна на сконтовия лихвен процент. Главно

средство за сконтовата политика есконтовия процент. Сконтовият процент същевременно ориентира стопанските субекти за намеренията на централната банка: повишаването на сконтовия лихвен процент означава, че централната банка ще провежда рестриктивна политика, и обратно-намаляването му е знак за стимулиране на стопанската активност чрез засилено парично предлагане.

Централната банка сконтира два вида търговски ценни книжа:

- ✓ издадени от търговските дружества или др. лица;
- ✓ издадени от самите търговски банки;

В нашата банкова практика преди валутния борд по-широко се прилагаха операциите с ценни книжа на ТБ. Търговската банка, която се нуждае от по-висока ликвидност, може да издаде запис на заповед, която да сконтира в централната банка и да покрие недостига на средства.

С) ***Операциите на открития пазар*** - те са основни икономически инструменти на централната банка за регулиране на паричната маса, паричния пазар и банковата ликвидност. Тяхната същност са покупко-продажбата от централната банка на правителствени или други ценни книжа.

Операциите на открития пазар могат да се изразят като окончателна покупка или продажба на ценни книжа, или като операции репо. Репо сделките са гъвкаво средство за регулиране на банковата ликвидност. Чрез операциите на открития пазар централната банка влияе непосредствено върху ликвидността на банковата система и паричното предлагане. Този инструмент на паричната политика има редица предимства:

- ✓ гъвкавост - операциите на открития пазар са много гъвкав инструмент за регулиране на банковите резерви и паричното предлагане;
- ✓ инициативност инициатор на тези операции е централната банка , докато при кредитирането инициативата е у търговските банки;
- ✓ осъществяват се доброволни транзакции;
- ✓ влияние върху кредитните операции - чрез изнемането на лихвените проценти те могат да се извършват както на първичните, така и на вторичните пазари;
- ✓ общоикономическо и общонационално значение - чрез тях може да се увеличава паричното предлагане и икономическата активност или, обратно;

Централната банка чрез продажбата на ценни книжа свива паричната база, намаляват се резервите на търговските банки и по този начин се свива паричната маса. Когато централната банка продава на населението ценни книжа, тя изтегля налични пари от обръщение, свива се паричното предлагане и се набалява инфлационната обезценка на парите. От м. юни 1997г. БНБ преустанови операциите на открития пазар с държавни ценни книжа при въвеждането на валутния борд.

Д) ***Норма на задължителните резерви*** - това е процент, който определя средствата, които търговските банки задължително съхраняват в централната банка. Определят се като норматив от общата сума на привлечените средства на търговските банки. В практиката са познати случаи, когато нормата на задължителните минимални резерви се определя и спрямо величината на предоставените кредити или спрямо сумата на активите на търговската банка. Операциите по задължителните резерви са също един класически инструмент на паричната политика на централната банка.

Като основно предимство на задължитерните резерви се очертава обстоятелството, че те влияят еднакво на всички банки. Промените в процента на задължителните резерви влияят върху паричното предлагане чрез кредитния мултипликатор. Този мултипликатор показва как може да нарасне първоначалният депозит вследствие на взаимните банкови операции, а оттук нарастват заемите и задължителните резерви.

*Е) **Ломбардни кредити на централната банка*** - с него се изразява предлагането на краткосрочни средства на търговските банки от централната банка. То се осъществява чрез отпускане на заеми на търговските банки срещу държавни и др. ценни книжа, скъпоценни метали и валута.

Лихвените проценти по отпусканите от централната банка заеми срещу залог на държавни ценни книжа трябва да бъдат по-високи от преобладаващите на паричния пазар лихвени проценти. В противен случай, търговските банки ще предпочетат да бъдат рефинансирани от централната бана. Залогът на ломбардните кредити се съхранява в централната банка до погасяването на заема.

*Ф) **Междубанкови депозити*** в определени случаи може да се провеждат и търгове за междубанкови депозити, чрез тях търговските банки може да си осигурят ликвидни средства. Търговските банки могат да предлагат на търга депозити само до размера на наличните си средства по разплащателната си сметка в централна банка, при условие, че са си попълнили задължетилните минимални резерви. Лихвения процент на разпределените краткосрочни депозити се определя от търсенето и предлагането, т. е. на пазарен принцип. Централната банка оказва влияние върху търсенето и предлагането като увеличава или намалява депозитите, които тя предоставя на търговските банки.

2.2.Същност на търговските банки

Търговски са банките, които търгуват с пари и капитали. Тяхната присъща дейност са паричните сделки. Те привличат разнообразни свободни капитали от икономиката и ги насочват към клиенти, които имат потребност от допълнителни капитали. Търговските банки са също предприятия, чиито основен продукт са услугите, свързани с посредничесвото, кредитирането, разплащанията. Чрез своята дейност банките се стремят да постигнат определени положетилни финансови резултати, тяхната основна цел е получаването на печалба. За разлика от другите стопански субекти, търговските банки имат особено място и са част от структурата на икономическите и управленските субекти. Те са субектите, които в най-голяма степен участват в процесите на движението на капиталите. Това възлово място в парично-кредитната система ги прави непосредствен участник в цялостния стопански живот на страната. От дейността на търговските банки са заинтересовани всички слоеве на обществото. В банките се кнцентрира значителна част от спестяванията на населението и натрупванията на фирмите, което формира доверието на субектите към националната парична единица.

Функциите на търговската банка намират реален израз в нейните разнообразни активни, пасивни и посреднически операции, които формират облика на банката, разкриват нейните позиции сред останалите банки от съответната банкова система, както и позициите й спрямо всички останали икономически субекти.

Икономическите функции са основа, те правят банката - банка, отделят я от останалите икономически субекти на обществено-икономическия субект. Това са дейностите по влогонабиране и кредитиране, разплащанията и обслужването на паричния оборот.

Търговските банки имат и управленски функции, които се реализират като:

- ✓ Управление на вътрешната структура на банката;
- ✓ Управление на дейността й извън банката;

Структурата на самата банка се управлява по вертикална връзка: от централата на банката към банковите клонове-фиалиалите-правителствата. Управление се осъществява и в отделните звена на търговските банки. Това са управленски функции, които са типични не само за банките, но и за всяка икономическа структура, за всяко икономическо звено или субект.

Организационно-управленската структура на търтавската банка може да се разглежда и анализира в два аспекта:

Вертикална структура изразява връзките и подчинеността между отделните банкови звена в системата на една банка от централата на ТБ към нейните клонове, филиали, агенции. От тази гледна точка управленската структура може да бъде: банка с клонова мрежа и банка без клонове.

Вътрешна структура зависи от юридическата форма на учредяването на търговската банка., най-често това са акционерни дружества. В някои страни се прилага едностепенна система на управление. При тази система управлението се осъществява от управителен съвет или борд на директорите. Когато е предвиден и надзорен съвет, тази система на управление на търговската банка се нарича двустепенна. В нашата страна Търговският закон дава възможност за прилагането и на двете системи - според решението на общото събрание на акционерите.

Класифицирането на търговските банки може да се основава на различни критерии като:

- ✓ източник за формиране на собствен капитал;
- ✓ правна форма;
- ✓ обслужвани клиенти;
- ✓ големина на основния капитал;
- ✓ срок на сделките;
- ✓ територия на функциониране;
- ✓ характеристика на дейността им;

Според източника за образуване на собствен капитал, търговските банки могат да бъдат:

- ✓ дължавни
- ✓ общински
- ✓ частни
- ✓ кооперативни

В нашата сегашна практика са регламентирани две форми за организиране на банковата дейност акционерна и кооперативна.

Според правната си форма търговските банки са три вида:

- ✓ еднолични предприятия;
- ✓ търговски дружества;
- ✓ кооперации;

Според характера на стопанската дейност на обслужваните клиенти търговските банки могат да бъдат определени като:

- ✓ промишлени
- ✓ търговски;
- ✓ земеделски;
- ✓ външнотърговски;

Според големината на основния капитал и на привлечените средства търговските банки могат да се разграничават условно на:

- ✓ големи;
- ✓ средни;
- ✓ малки;

Според териториалния обхват на дейността им търговските банки биват:

- ✓ национални;
- ✓ регионални;
- ✓ чуждестранни;
- ✓ транснационални;

Според операциите, които осъществяват, търговските банки могат да се разграничават на:

- ✓ специализирани;
- ✓ универсални;

Към специализираните търговски банки се отнасят:

- ✓ ломбардните банки;

- ✓ ипотекарните банки;
- ✓ инвестиционните банки;
- ✓ депозитно-спестовните банки;
- ✓ джиро-банките;
- ✓ депозитно-кредитните банки;
- ✓ сконтовите банки;

Най-разпространени са универсалните банки. Те извършват всички видове операции като:

- ✓ кредитиране;
- ✓ разплащания;
- ✓ доверителни операции;

Според обхвата на дейността си универсалните търговски банки биват:

Напълно универсални. Извършват не само традиционната банкова дейност, но и търговия с ценни книжа и застрахователна дейност. Такива банки се срещат в Швейцария, Германия, Холандия.

Английска форма на универсалните банки. Тук по-рядко се комбинира банкова и застрахователна дейност, както и между банкови операции и такива с ценни книжа.

Американски тип универсални банки. Те не могат да притежават акции на частни предприятия и корпорации. Покупка на ценни книжа на нефинансови предприятия могат да извършват само холдинги и националните банки.

Японските универсални търговски банки са подобни на тези от САЩ при тях също има законодателно разграничаване между пряката банкова дейност и търговията с ценни книжа.

Търговските банки осъществяват парично, платежно, кредитно и капиталово посредничество на своите клиенти, чрез многообразните си операции. От позициите на банковия баланс операциите се разграничават на два вида: активни и пасивни.

В пасивните операции на търгавските банки се включват операциите по формирането на собствения капитал и операциите по мобилизирането на чужди средства. Основна операция на всяка търговска банка, с която практически се започва, е формирането на собствения капитал. Банката може да получи лиценз, само при положение че е образуван регламентираният размер на собствения капитал. В паричните операции на търговските банки съществено място заемат кредитите, които те получават от паричния пазар. Нефинансовите субекти кредитират банките, когато закупуват емитирани от тях собствени облигации и чрез депозитните сертификати.

При осъществяване на активните операции търговските банки се стремят да повишават своята рентабилност и ликвидност. Затова основен подход тук е всяка банка да има възможност да посреща ежедневно задълженията си към клиентите и всички кредитори. Кредитните операции са най-съществената част на активните операции на търговските банки. Същевременно кредитите са и най-малко ликвидни, те са най-рискованият актив на банките. Поради това всяка търговска банка се стреми да диверсифицира кредитния си портфейл чрез предоставяне на кредити с различна степен на риск. Освен това по този начин се осигурява и ритмичното формиране на доходите на банките.

Комисионните операции на търговските банки са третият вид банкови операции. При тях банките не ангажират собствен капитал. Те извършват услуги на своите клиенти, срещу което получават доход под формата на такси, комисионни и др. подобни плащания. Такива операции са:

- ✓ преводни, акредитивни, инкасови;
- ✓ доверителни;
- ✓ емисия, покупко-продажба на ценни книжа;
- ✓ покупко-продажба на валута;
- ✓ анализи, информация, прогнози по поръчка на клиенти;

В съвременното банково дело тълкуването на банковите услуги е много по- широко. Всичко, което банките предлагат на своите клиенти при определена цена, се обозначава като банкова услуга. Така в съвременното разбиране на понятието банкови услиги се включват: кредитирането, влогоговите операции, сделките с ценни книжа, разплащанията, управлението на имущества, посредничество в застрахователните операции, консултациите, електронната обработка на данни.

Всяка търговска банка се стреми да получава конкурентни предимства члез широчината на чадъра от банкови услуги или чрез високо качество на по-малко, но специализирани услуги.

2.3.Видове организационно-управленски структури в Търговските Банки

При обслужването на своите клиенти търговските банки могат да изберат една от множеството организационни структури, която трябва да е обвързана с характера на стратегическата ориентация на банката по отношение на нейната основна дейност. В универсалните банки съществуват основни дирекции и отдели, занимаващи се с осъществяването на традиционни и модерни банкови услуги, но като цяло организационните структури на кредитните институции не си приличат.

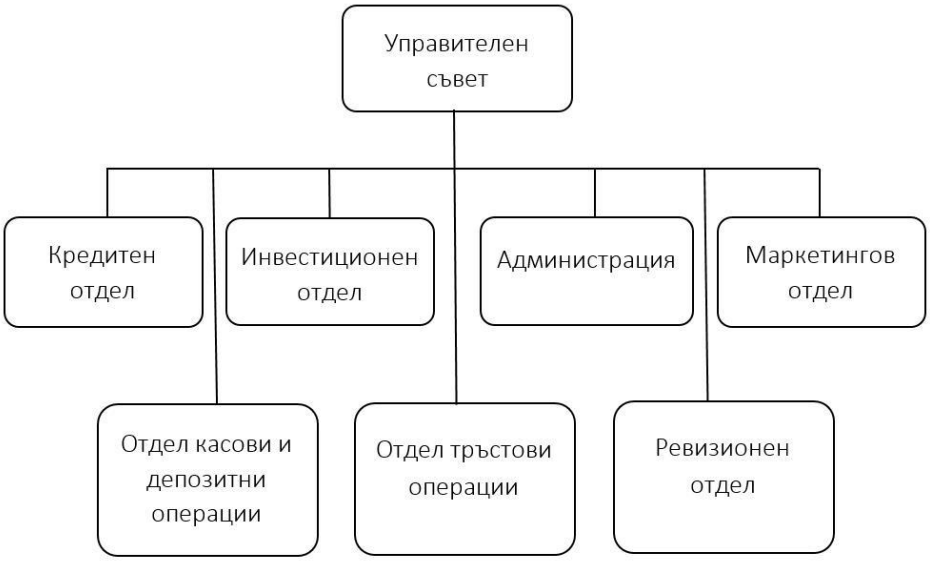
Функционирането на банката става в рамките на организационната й структура. Тя обхваща подредените в йерархичен ред основни звена в кредитната институция – управления, дирекции, отдели, а също и органите за управление и надзор на банката.Взаимодействието между отделните звена на кредитната институция осигурява процеса на функциониране и развитие на банката като единна система.

Някои автори разграничават организационната структура на банката от нейната управленска структура. Към звената на последната се отнасят органите за управление на банката (общо събрание, управителен съвет, надзорен съвет) и ръководителите на всички подразделения.

Съществуват различни видове организационни структури. Най-често срещаните са функционална, дивизионална и организационна структура на банки, действащи на международните пазари.

2.3.1.Йерархическа организационна структура

За малките по размер банки, опериращи на даден локален пазар на банкови продукти и услуги, които обслужват ограничен контингент от клиенти, които не са изложени на силен конкурентен натиск и не разполагат с развита клонова мрежа, е подходяща т.нар. йерархическа организационна структура. Тя се характеризира с простота на вертикалните връзки и пряко подчинение на отделите на висшето банково ръководство (виж фиг. 08).

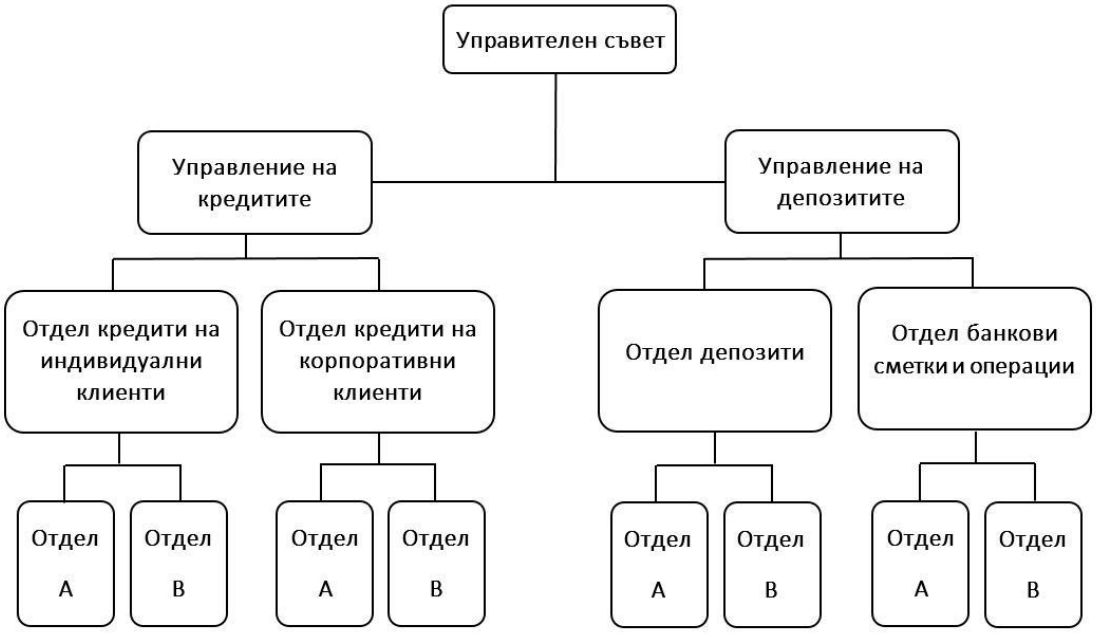


Фиг. 08. Йерархическа структура на банката

2.3.2.Функционалната организационна структура

Изисква банката да се структурира в зависимост от типичните функции, които изпълнява: кредитни сделки (commercial banking), сделки на паричните и капиталовите пазари (investment banking), управление на имуществото и капитала (trust banking) и логистика. Всички тези функционални поделения са подчинени на оперативното ръководство на банката. Някои от тях обаче могат да имат и известна самостоятелност, например да бъдат центрове на печалбата (profit centers) и да контролират печалбите и загубите, както и да следят за величината на рентабилността на собствения капитал.

Подкрепящите дейности се осъществяват от спомагателни служби, които функционират като центрове на разходите (cost centers). Те разпределят средствата към сферата на търговското и инвестиционното банкиране.Така тази организация разкрива възможност за създаване на "банки в самата банка" или суббанки. Всяка суббанка е център на печалбата или на инвестициите, като има свой осигуряващ разходен център, който би могъл да "търгува" с другите центрове. Функционалната структура се прилага в по-малки банки, които обаче са способни да действат самостоятелно в пазарни условия (виж фиг. 09).



Фиг. 09. Линейно-функционална структура на банката

Функционалният тип организация на вътрешнобанковите подразделения е традиционен. Подобен принцип на организация, ако е структуриран подходящо, осигурява определени конкурентни преимущества, свързани със задълбочаване на специализацията, надеждност на комуникациите, повишаване качеството на предлаганите банкови услуги, отсъствието на дублиране, което позволява да се вземат оперативно и да се реализират успешно необходимите управленски решения.

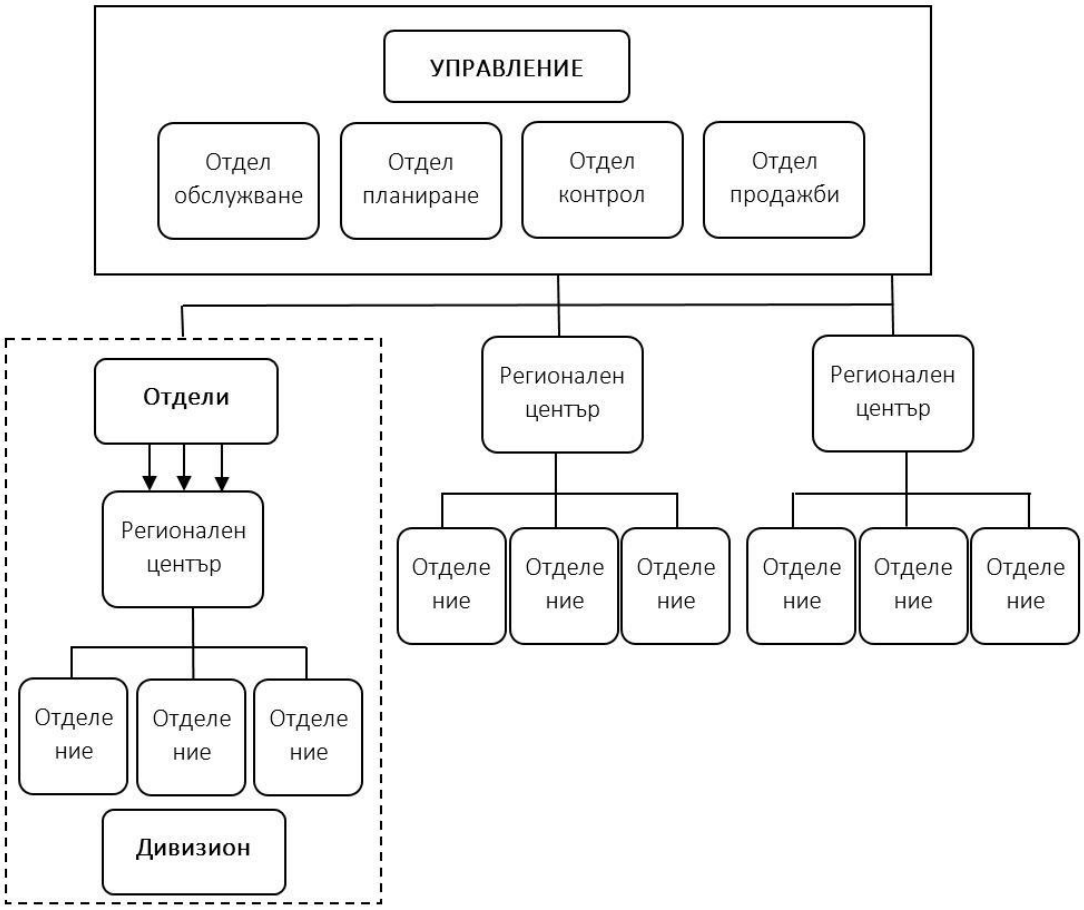
Линейно-функционалната структура на банковите институции има редица недостатъци, които не им позволяват да се приспособяват бързо към постоянно променящите се условия на пазара, но основният се състои в затрудненото движение на информацията. То е свързано както с хоризонталните връзки и комуникации (когато ръководителите и специалистите от даден отдел не могат да разберат проблемите на другите отдели), така и с вертикалните (когато ръководителите на отделните дирекции, звена и отдели дават противоречиви указания и задачи на подчинените им банкови служители). В такива структури решенията се приемат бавно и тяхното качество се определя не толкова от компетентността на самите ръководители, колкото от надеждността и достоверността на постъпващата към тях

информация. От друга страна банковите служители, заемащи ръководни длъжности в подобен тип организационни структури, се стремят да поемат възможно по-малък риск при вземането на дадено важно решение и не се стремят да не поемат големи отговорности.

2.3.3.Дивизионална организационна структура

Тя предполага разделяне на банката не по функции, а в съответствие с видовете банкови продукти, клиентите на банката или по регионален признак. В първия случай се прилага в банки, които осъществяват продажби на широк асортимент продукти и услуги и затова е необходимо да се обособи отделно ръководство за всеки предоставян вид услуга. То отговаря за въвеждането на нови продукти и за повишаване качеството и продажбите на вече съществуващите.

Във втория случай банката съсредоточава вниманието си върху определени групи клиенти – корпоративни, индивидуални, дребен и среден бизнес, а ако е универсална и по-голяма – върху всички групи потребители. Регионалните организационни структури се срещат при банки, които оперират в по-широк географски район. Целта е пълно обхващане и обслужване на клиентите по отделни области и региони с отчитане на местните особености (виж фиг. 10).



Фиг. 10 Дивизионална (регионална) структура на банката

Дивизионалната структура на банката създава благоприятни възможности за приемането на по-ефективни и адекватни на реалността решения, основани на по-добро познаване на местните условия, като по този начин висшето ръководство се разтоварва от необходимостта за осъществяването на постоянен контрол върху оперативната дейност на отделните структурни звена. От друга страна обаче при дивизионалната структура на банката се създават предпоставки за дублиране на отделните управленски функции поради раздуването на управленския апарат, но в повечето случаи нарастването на административните разходи е оправдано с оглед повишаването на конкурентоспособността и

гъвкавостта на институцията в условията на динамично развиващия се пазар на банкови продукти и услуги.

2.4.Организационната структура на банките, действащи на международните пазари

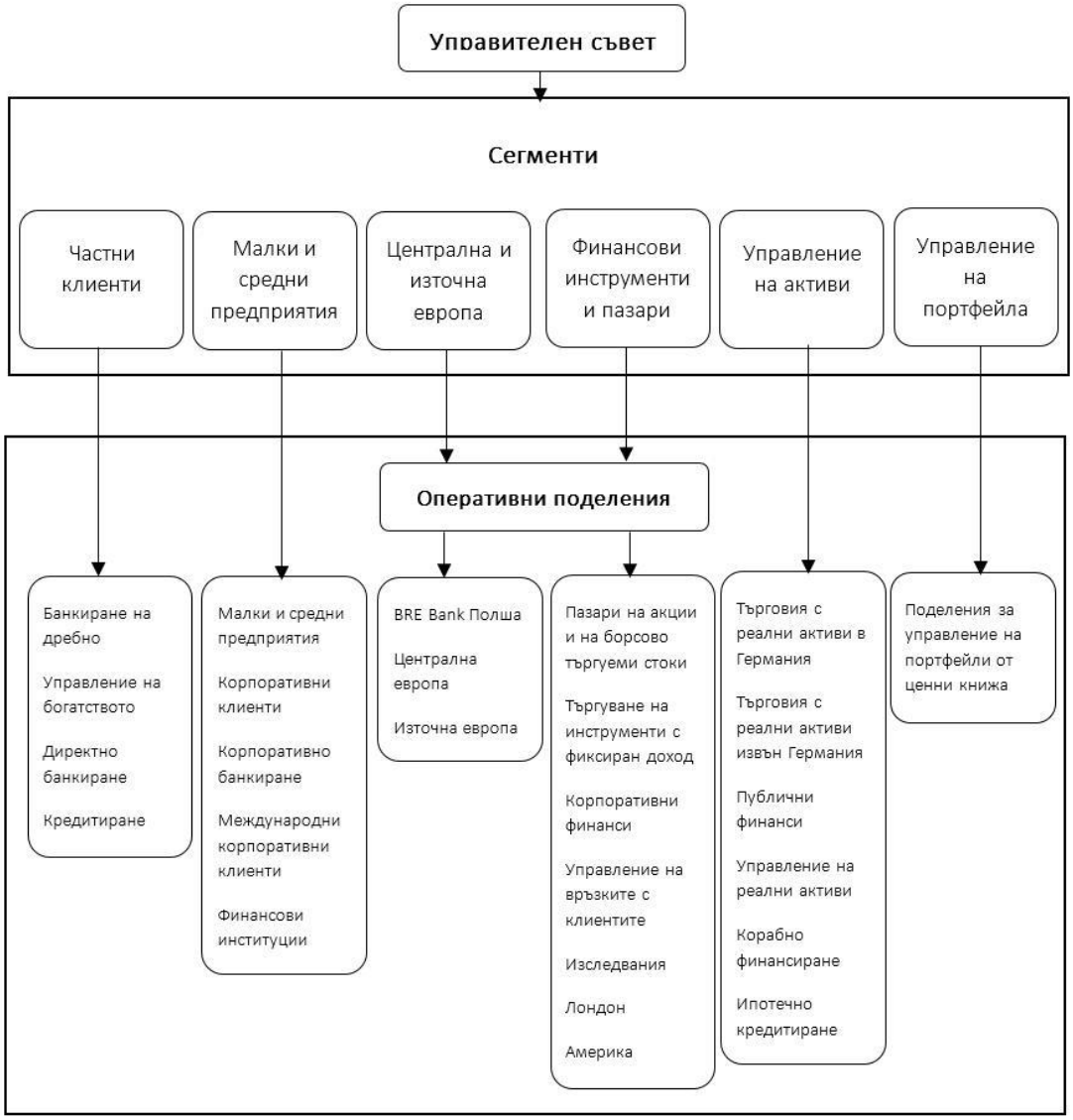
Тя също може да се ориентира по региони или по продукти. В глобален аспект банката може да извършва дейност в 4 организационни форми – поделение, представителство, филиал или да има консорциално участие.

Срещат се и три вида адаптивни организационни структури – проектни, матрични и конгломерати. ***Проектните*** се прилагат при решаването на конкретни задачи, като внедряването на нова управленска система или електронно банкиране. На ръководителите на тези проекти се предоставя временно относителна самостоятелност. ***Матричните*** позволяват да се обединят предимствата на функционалната и дивизионалната структури и да се постигне по-голяма гъвкавост и ефективност. ***Конгломератите*** са обединения от няколко структури, позволяващи на така обособената мегабанка да реагира адекватно на пазарната среда, включително и чрез покупко-продажба на по-малки банки, които са съставна част от конгломерата.

С разширяването на банковата дейност на националните и международните пазари в условията на постоянно нарастваща междубанкова конкуренция, с непрекъснатото въвеждане на нови продукти и услуги, с развитието на информационните технологии и увеличаването на клиентската база, която трябва да се обслужва все по-качествено и комплексно от висококвалифицирани специалисти и експерти, се поражда необходимостта от създаването на нов тип организационни структури. Така например от 1956 година в САЩ функционират банкови холдингови компании. Те са юридически лица, които директно или индиректно притежават, контролират или управляват повече от 25 % от акциите на американски банки. От своя страна тяхната дейност се контролира от федералната резервна система на САЩ. Те могат да се преобразуват и във финансови холдингови компании. Във Великобритания също функционират десетки банкови холдингови компании, които играят съществена роля за развитието на банковия сектор както в страната, така и в глобален аспект.

Организационно-управленска структура на банков концерн

В Германия и немскоговорящите страни и Прибалтика се използва друга терминология за холдинговите структури – те се наричат банкови концерни. Типично за концерна е съхранението на юридическата и икономическата самостоятелност на участниците в него, като доминираща и координираща роля обикновено има дадена водеща търговска банка.

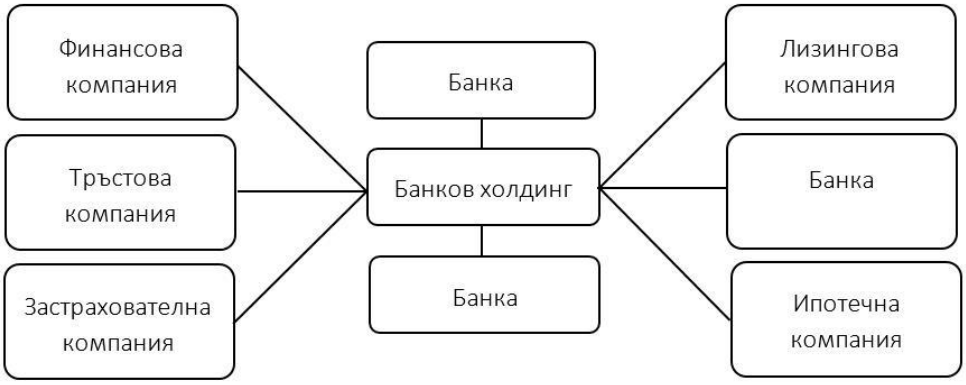


Фиг. 11 Организационна структура на банков концерн от Германия

От представената на следващата фиг.11 организационна структура на действащ банков концерн от Германия става ясно, че пазарът, на който той оперира, е сегментиран както по клиентски, така и по географски и продуктов признак. В структурата му са включени и контролираните банкови институции, осъществяващи своята дейност на националния и на международния пазари.

Организационно-управленска структура на банков холдинг

През последните години банковите холдинги започнаха да включват във своята структура различни небанкови финансови институции, които са тясно свързани с банковата дейност – лизингови компании, застрахователни, пенсионноосигурителни и здравноосигурителни дружества, финансови, одиторски и инвестиционни дружества и т.н. Целта на подобен тип организация е да се обхванат максимално широк кръг от клиенти, ползващи различни банкови и финансови услуги и да се извърши комплексното им обслужване „под един покрив” (виж фиг. 12).



Фиг. 12 Холдингова организационна структура на банката

Структурата на банковите подразделения (дирекции, отдели, звена) може да варира в широки граници и да се класифицира по различни признаци.

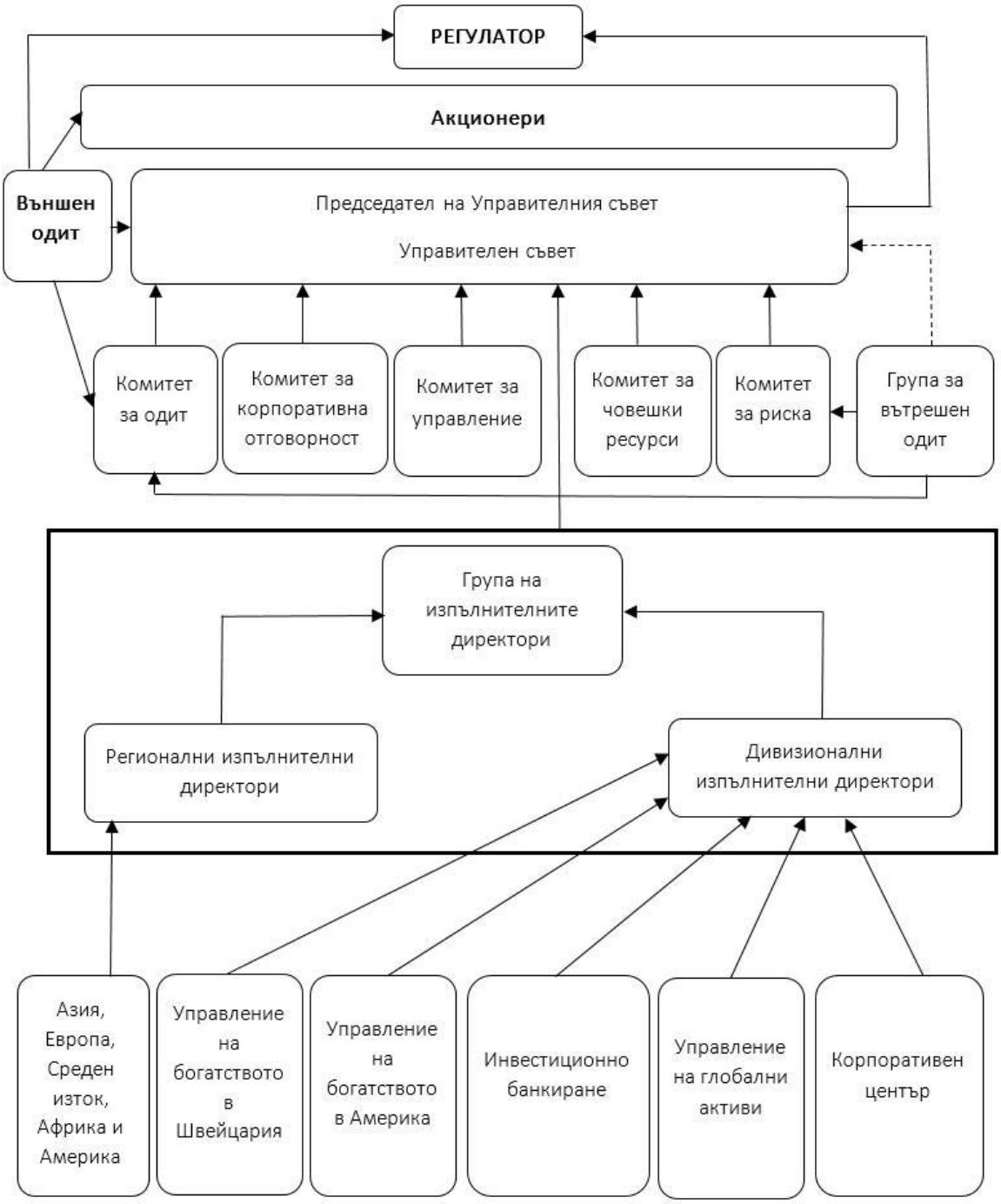
От гледна точка на тяхната организационната структура подразделенията на универсалните банки могат се причислят към някой от следните два основни типа.

Икономически – подразделения за кредитиране, за извършване на влогонабирателни операции, за извършване на платежни и касови операции, за работа с клиенти, за валутни операции и външнотърговска дейност, за ценни книжа, за работа с персонала, за обслужване на банкови карти, за стратегическо развитие и планиране дейността на банката, за анализ на банковите рискове, за маркетинг и реклама и др.

Инфраструктурни – счетоводство, деловодство, вътрешен контрол, подразделения за безопасност и сигурност на информацията, за юридически услуги, за информационни технологии, за административно-стопанско обслужване.

Организационна структура на действаща на глобалния пазар европейска търговска банка:

На следващата фиг. 13 е представена организационна структура на действаща на глобалния пазар европейска търговска банка. Начело на банката стои Управителен съвет, избран от Общото събрание на акционерите. Отделните членове на Управителния съвет отговарят за съответни направления или функционални дейности, както и за части от клоновата мрежа, разпределени по териториален признак.



Фиг. 13 Организационна структура на европейска банка, опериращa на международните пазари

Към банката има изградени звена за външен и вътрешен одит, които контролират дейността на Управителния съвет и подчинените му комитети. Изпълнителните директори осъществяват оперативното ръководство на подчинените им дирекции, разграничени по регионален и функционален признак. Комитетът за одит се състои от трима членове на Управителния съвет (Борд на директорите), които извършват обективен контрол и надзор на провежданата счетоводна и финансова политика на банката. Те оценяват по-конкретно ефективността на управлението на риска и на процеса на контрол върху регионалните и функционалните звена, ефективността на вътрешния контрол, надеждността и достоверността на финансовата и оперативна информация, както и съответствието на дейността с нормативните и регулаторни изисквания.

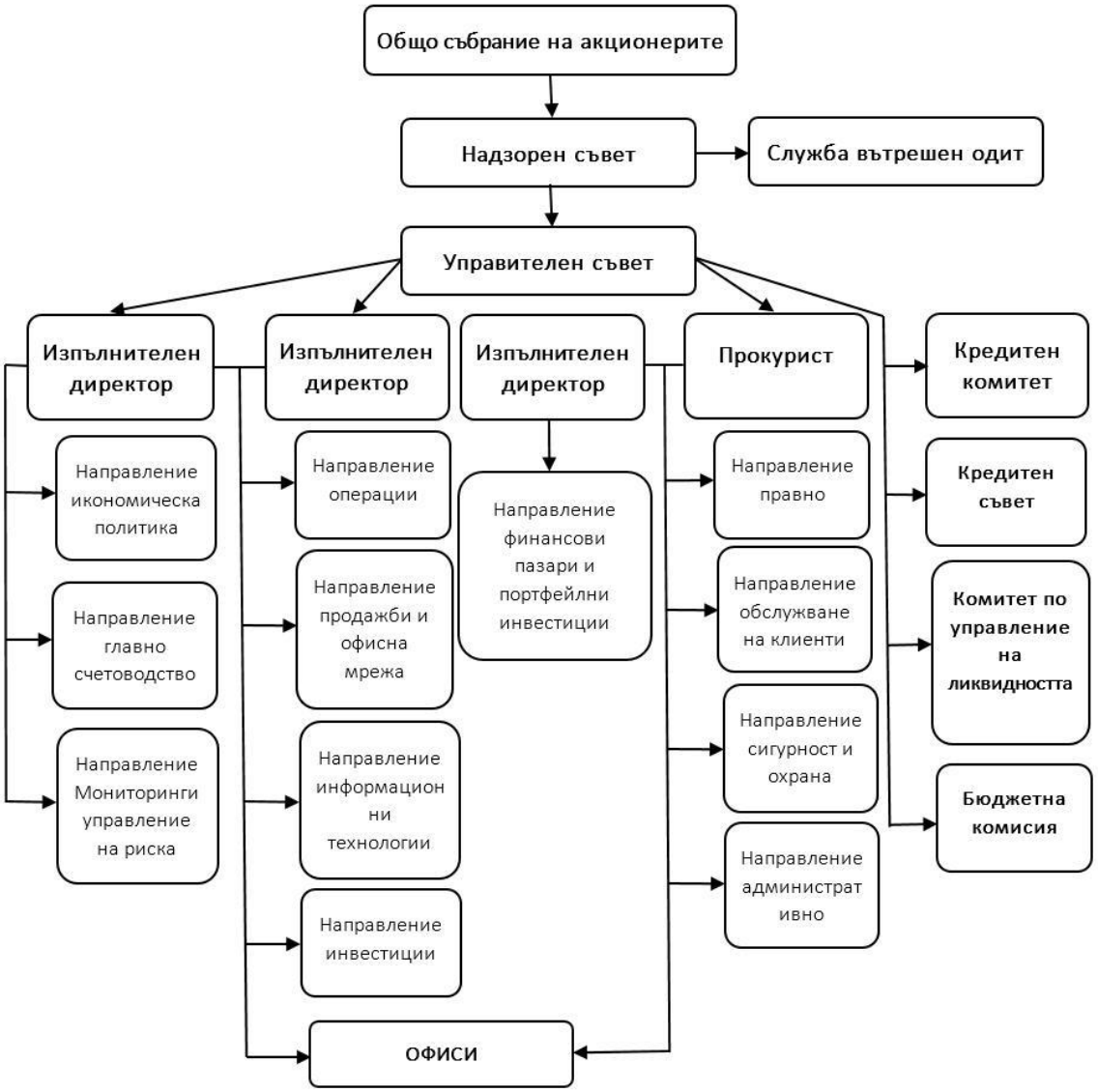
Комитетът за корпоративна отговорност е упълномощен да следи за ефективността на комуникационната политика на банката, да направлява и налага определена корпоративна

култура, да избягва и предотвратява такива негативни явления като корупцията, прането на пари и финансирането на тероризма, да повишава имиджа на институцията и др.
Функциите на комитета за управление са да подкрепя налагането на добри практики в корпоративното управление, да номинира нови членове на борда на директорите, да оценява тяхната дейност и да ги обучава по специализирани образователни програми.
Функциите на комитета за човешки ресурси са да утвърди подходяща система за стимулиране и компенсиране труда на банковите специалисти, да проучва внимателно състоянието и потребностите на административния и щатен персонал и да определя възнагражденията на членовете на съвета на директорите.

Комитетът за риска трябва да надзирава спазват ли се принципите и как се осъществява контрола в областта на управлението на кредитния, пазарния и операционния рискове, спазват ли се капиталовите изисквания и изискванията за ликвидност и как те се отразяват върху банковия баланс.

2.5.Организация на управлението на банковата дейност на кредитните институции, осъществяващи своята дейност в България

Тя не е много по-различна от тази на западните банки. На следващата фиг. 14 е представена организационна структура на една от банките, опериращa на местния пазар.



Фиг. 14 Организационна структура на търговска банка, опериращa на българския пазар на банкови услуги

Дейността на банката се осъществява чрез офиси и изнесени работни места. Органите за управление на банката са Общо събрание на акционерите, Надзорен съвет и Управителен съвет. Към надзорния съвет е създадена специализирана служба „Вътрешен одит". Към Управителния съвет са създадени следните постоянни помощни органи – Кредитен комитет, Кредитен съвет, Комитет по управление на ликвидността и Бюджетна комисия, които функционират по утвърдени от УС правила. [8]

Общото събрание - свиква се на редовно заседание веднъж годишно, но не по-късно от края на първото полугодие и може да:

- Изменя и допълва Устава на банката;
- Решава въпросите, касаещи увеличението и намалението на капитала на банката;
- Взема решение за обезсилване на акции, като определя и реда за това;
- Преобразува и прекратява банката;
- Избира и освобождава членовете на Надзорния съвет и определя възнагражденията им;
- Избира и освобождава ръководителя на службата за Вътрешен одит;
- Избира и освобождава специализирано одиторско предприятие;
- Одобрява годишния финансов отчет;
- Приема годишния доклад за дейността на банката, представен от Управителния съвет;
- Освобождава от отговорност членовете на Надзорния съвет и на Управителния съвет;
- Назначава ликвидаторите при прекратяването на банката, освен в случай на несъстоятелност;
- Решава и други въпроси, предоставени в неговата компетентност със закон или с устава на банката.

Надзорният съвет - състои се от трима до пет членове, които се избират от общото събрание за срок до 5 години и могат да бъдат преизбирани без ограничение. Те не могат да бъдат едновременно и членове на Управителния съвет на банката. Надзорният съвет:

- Не участва в управлението на банката;
- Одобрява правилника за работа на Управителния съвет;
- Избира членовете на Управителния съвет и определя техните възнаграждения;
- Овластява двама или повече членове на Управителния съвет, наричани изпълнителни директори, да представляват банката;
- Одобрява прокуристи и търговски пълномощници;
- По всяко време може да изисква сведения и доклади по въпроси, засягащи банката;
-Заседава най-малко веднъж на три месеца.

Управителен съвет - в някои ТБ над управителния съвет стои контролен съвет. Състои се от 3 до 5 лица, избрани за срок до 5 години. Членовете му могат да бъдат преизбирани без ограничения. Управителният съвет, с одобрението на Надзорния съвет избира измежду членовете си най-малко двама изпълнителни директори, като ги овластява да управляват банката и да я представляват. Изпълнителните директори могат да упълномощават трети лица за извършване на отделни действия. Те могат да упълномощават прокуристите да представляват банката. Управителният съвет:

- Организира изпълнението на решенията на Общото събрание и на Надзорния съвет;
- Приема програми, бюджет и оперативни планове, касаещи дейността на банката;
- Определя структурата и длъжностите в банката;
- Изготвя и предлага за одобрение от Надзорния съвет годишния финансов отчет и предложението за разпределение на печалбата, което ще направи пред Общото събрание на акционерите;
- Решава въпроси по кредитната и лихвената политика на банката, по размера на таксите, комисионите и разноските, които банката събира по операциите си;
- Взема решение за предоставяне на големи и вътрешни кредити;
- Приема правилник за работата си, който се одобрява от Надзорния съвет;
- Приема вътрешно нормативните актове на банката;
- Изпълнява и други функции, възложени му от Общото събрание и Надзорния съвет.

Управителният съвет, изпълнителните директори и прокуристът отговарят за дейността на отделните направления, които са им подчинени. Те са следните:

- Направление „Икономическа политика”
- Направление “Главно счетоводство”
- Направление “Мониторинг и управление на риска”
- Направление „Операции”
- Направление „Продажби и офисна мрежа”
- Направление „“Информационни технологии”
- Направление “Инвестиции”
- Направление „Финансови пазари и портфейлни инвестиции”
- Направление “Правно”
- Направление “Обслужване на клиенти”
- Направление „Сигурност и охрана”
- Направление “Административно”

Банката има изградена клонова мрежа, състояща се от десетки офиси, разположени по територията на цялата страна, в които работят стотици банкови служители.

Съществуват и съвещателни органи, в които се привличат специалисти извън системата на банката.

1) Централни дирекции - Секретариат към Управителния съвет - води кореспонденцията на ръководството; Правна дирекция - урежда юридически проблеми, подготвя крупни консорциални договори, взема мерки за отстраняване на рисковете в банковата работа; Организационна дирекция - тя е централен орган за направляване дейността на банката; Ревизионна дирекция - упражнява текущ контрол в/у дейността на банката; Дирекция Персонал- занимава се с кадрите в банката и въпросите свързани с рационалното разпределение на банковите служители, тяхното назначаване, преместване, уволняване; Дирекция Икономическа - събира, анализира, обработва и публикува данни за икономическото, финансовото, валутно състояние и дейността на самата банка; Дирекция Статистическа- обработва и обобщава данни за вътрешно-банковата работа в количествен и стойностен разрез.

2) Оперативни отдели I степен - това са отдели, които извършват текущата банкова дейност. Такива са: касовия отдел, отдел преводи, отдел чекове, отдел менителници, отдел ценни книжа, валутен отдел, депозитен отдел, кредитен отдел.

3) Оперативни отдели II степен - се считат звената, които отразяват счетоводно, статистически и оперативно дейността на банката. Такива са: Отдел Прима нота; Отдел Главно счетоводство; Отдел Електронна обработка на информацията; Контокорентен отдел.

4) Спомагателни отдели - те създават условия за нормална работа в дирекциите и оперативните отдели.

От представените досега организационни структури на банката става ясно какви са предимно вертикалните връзки и зависимости между отделни нейни звена. В следващото изложение ще бъде направен опит да се изясни какво представляват и как се изграждат хоризонталните връзки между подразделенията на отделните кредитни институции.

Хоризонталните връзки се осъществяват във вид на обмен на знания, технологии, идеи, оценки, документи и текуща информация между отделните банкови подразделения. Формите на взаимодействие се избират на основата на конкретните изисквания на практиката и в съответствие с интересите на всеки сътрудник. Известно е, че почти всички банкови подразделения не разполагат с достатъчна като обем, достоверност и качество информация. Част от банковите специалисти не са запознати с цялостната дейност на банката и с дейността на останалите отдели. Ето защо всеки отдел трябва да определи каква информация, в какъв вид и с каква периодичност трябва да му се предоставя от останалите подразделения. Структурата на информационните потоци следва да се уточнява и коригира регулярно.

Обменът на информация не трябва да се състои само от обмен на документи с текущ характер или въвеждане на файлове в компютърната мрежа. Не по-малко важно е да се обменят данни с аналитичен и прогностичен характер. От друга страна специалистите от даден отдел могат да предоставят на останалите подразделения ценна информация, която да им позволи да работят в синхрон и да постигат по-висока ефективност. По този начин управлението на банката става по-гъвкаво и крайните резултати от нейната дейност могат да се подобрят значително. Добър подход в това отношение може да бъде периодичното събиране на ръководителите на отделните звена и отдели с представители на централното ръководство на банката, като всеки от тях излага своите виждания, оценки и идеи в следните направления: какви проблеми съществуват в съответното подразделение, как тези проблеми се отразяват на дейността на останалите подразделения, какви външни фактори предизвикват трудности в работата на съответния отдел, на останалите отдели и на банката като цяло и кои са възможните методи и средства за решаването на тези проблеми. Подобни обсъждания могат да се правят и в рамките на самия отдел, като целта е да се идентифицират проблемите, които възникват и да се вземат възможно най-подходящите решения за тяхното отстраняване.

2.6.Организационна структура и органи за управление на централните банки

След като се изясниха особеностите, спецификата и разновидностите на организационните структури, по които е изградена дейността на търговските банки, е необходимо да се проследи по какъв начин са изградени организационните структури на централните банки.

В съвременния си вид Централните банки съществува повече от три столетия. Счита се, че първата централна банка в света е била Шведската държавна банка "Свиригес Риксбанк" основана през 1668 г. За основоположник на двузвенната банкова система се приема Английската банка, създадена през 1694 г като емисионен институт с частен акционерен капитал.

Форма на организация на Централната Банка

В света има 2 модела за изграждане на Централната банка. При първия модел ЦБанка така е организирана че провежданата от нея парично- кредитна политика цели изпълнение на задачите поставени й от правителството. Втория модел на организационно изграждане на Централната Банка е независима от полтическата власт и изпълнява строго определени икономически задачи чрез използването на специално предназначени инструменти. Една от основните цели, които си поставя такава ЦБ е поддържането на стабилни вътрешни цени или валутен курс.

Българска народна банка

Органи за управление на Българската народна банка (БНБ) са управителният съвет, управителят и трима подуправители. Управителният съвет се състои от седем членове и включва в своя състав управителя и трима подуправители, които се избират от Народното събрание, както и други трима членове, които се назначават от Президента. Мандатът на членовете на управителния съвет е шест години и при определени условия може да бъде прекратен предсрочно.

Основни задачи на Централните банки

В края на XX век и началото на XXI век Централните банки са юридически лица, които имат определени със закон функции и задачи. Естествено е те да са единствените емисионни центрове, т.е. тяхната основна функция да е емисионната. Освен това те се грижат за стабилността на паричнита единица, за провеждането на адекватна на икономическото положение в страната парично-кредитна политика, имат контролни функции по отношение на търговските банки, грижат се за ефективността на платежните механизми в страната. За да изпълни основните си задачи Централната Банка трябва да има определена степен на независимост от изпълнителната власт- политическа и икономическа. Политическата се

свързва с влиянието на правивителството върху политиката на банката, автономията при определянето на целевите ориентири на паричното предлагане и паричната маса. Икономическата независимост се свързва със: способността на правителството да определя условията на кредитиране от Централната Банка и множеството парични инструменти с които тя разполага.

2.7.Организационно устойство и компетенции на БНБ

Основните и функции се разделят на три вида: регулиращи, контролни и обслужващи.

Регулиращи:

1)управлението и контрола върху паричната маса и паричното предлагане
2)регулиране на паричната сфера
3)регулиране на търсенето и предлагането на кредити.

Контролни:

1)лицензиране на новосъздадените банки
2)текущ контрол
3)въвеждане на валутен контрол.

Обслужващи:

1)организация на систематамата в сферата на разплащанията
2)кредитиране на ТБ
3)изпълняване ролята на финансов агент на правителството.

Към допълнителните функции могат да се посочат: управление на държавния дълг, провеждане на анализи, икономически и статистически изследвания, емисия на банкноти и контрол върху циркулацията им на територията на страната.

Основна задача на Централната банка - да поддържа стабилността на националната парична единица чрез провеждане на парична и кредитна политика, да съдейства за създаването и функционирането на ефективни платежни механизми.

Управления на БНБ - в БНБ са създадени три основни управления – „Емисионно", „Банково" и „Банков надзор", като има и едно допълнително – „Фискални услуги". Всяко от тях се ръководи пряко от подуправител, избран от Народното събрание.

Управление „Емисионно" - основната функция на управление „Емисионно" е да поддържа пълно валутно покритие на общата сума на паричните задължения на БНБ, като предприема необходимите действия за ефективно управление на брутните международни валутни резерви на банката.

Организационната структура на управление Емисионно е следната: 3 дирекции - "Касова" "Ковчежничество" и "Анализ и контрол на риска". Към дирекция "Касова" са отделите: "Резервна маса", "Банкноти и монети" и "Касови технологии". Към "Ковчежничество": "Анализ", "Инвестиции" и "Ликвидност". И към дирекция "Анализ и контрол на риска": "Анализ на риска", "Контрол на риска" и "Касов риск".

Управление „Банково" - при определени условия управление „Банково" изпълнява функциите на кредитор от последна инстанция при възникването на системен риск за банковата система.

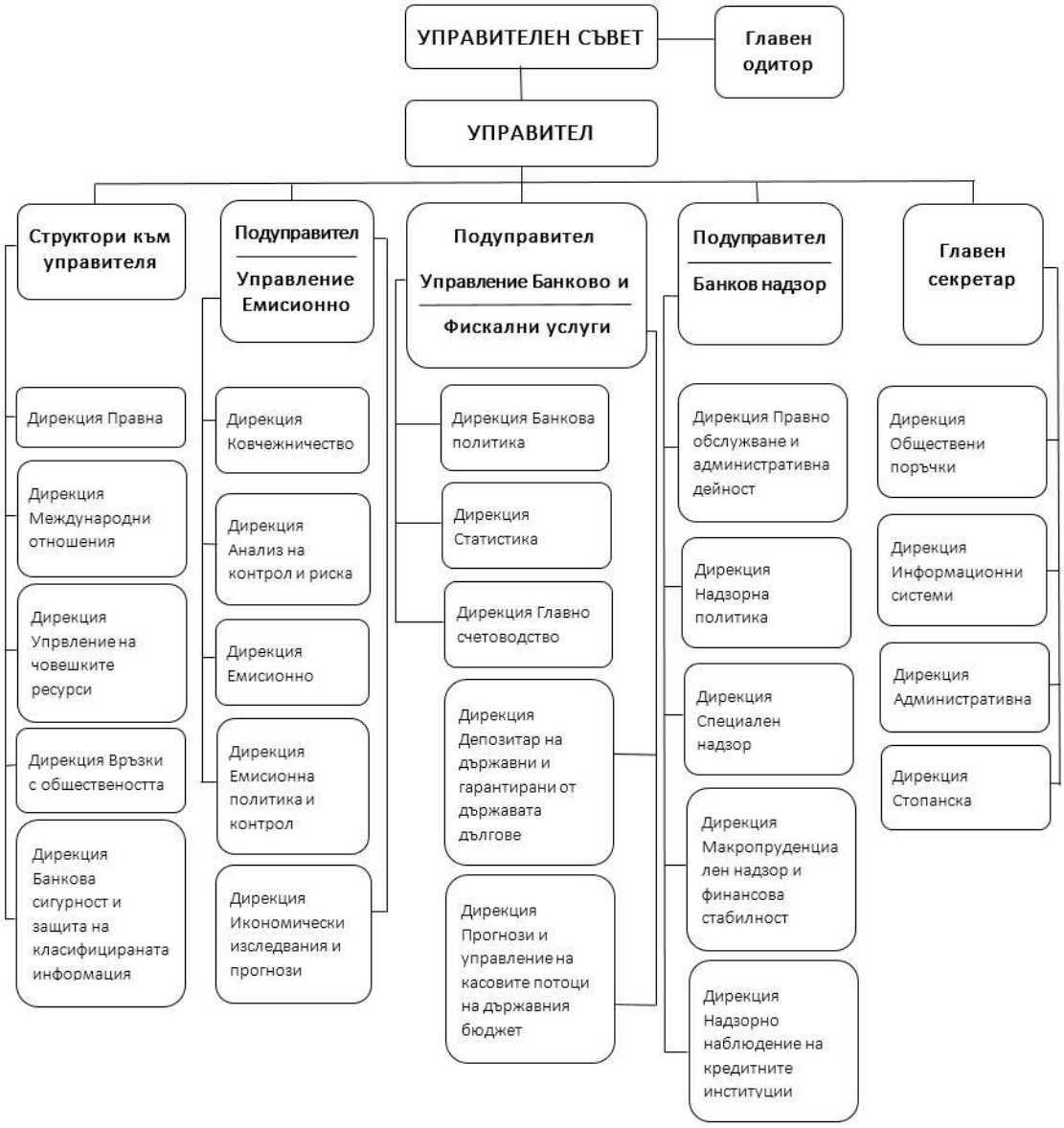
Основна негова задача е да изпълнява фукцията на кредитор от последна инстанция в случай на системен риск, заплашващ стабилността на банковата система. По конкретно това управление: 1)предоставя левови кредити на Търговски банки 2) анализира състоянието на Търговските банки 3) осъществява контактите на БНБ и другите междунар финансови институции 4) извършва операциите по касовото изпълнение на държавния бюджет 5) съставя платежен баланс на страната 6) изготвя анализ на паричната статистика. Управление

“Банково” има 5 дирекции – “Банкова политика”,”Международни отношения и европейска интеграция”, ”Икономически изледвания и прогнози”, ”Статистика” и “Главно счетоводство”.

Управление „Банков надзор” - осъществява надзора върху банковата система съгласно определени нормативни актове. БНБ в лицето на управление „Фискални услуги” действа като фискален агент, агент по държавните дългове и депозитар на държавата.

По конкретно правомощията на това управление се свързват с: лицензиране на новооткрити банки; осъщесвяване на текущ контрол и надзор върху търговските банки. На практика в дейноста на банковия надзор се забелязват две относително самостоятелни, но същевременно и парично следствени фази: 1)контролно - установителна фаза - цели се събирането на максимално достоверна задоволотелна информация за наблюдаваните субекти. 2)фаза на надзорно въздействие - на базата на събраната от предходната фаза информация се възприемат определени мерки спрямо проверяваните лица. Управление Банков надзор се състои от 5 дирекции: ”Надзорна политика и методология”, ”Специален надзор”, ”Дистанционен надзор и анализ”, ”Инспекции” и “Надзорна администрация.

Управление Фискални услуги - в организационната структура на БНБ има още едно управление “Фискални услуги” което не е основно. Чрез него се осъщесрвяват отношенията между БНБ и държавата, в онази им част, в която БНБ действа като агент по държавните дългове или по дългове гарантирани от държавата. [8]



Фиг. 15 Организационна структура на БНБ

Главният одитор, избран от управителния съвет на БНБ, осъществява вътрешния одит в банката. Той следи за качеството на системите за вътрешен контрол и за управление на риска и съдейства на ръководството на банката за тяхното усъвършенстване. Към управление „Емисионно" на БНБ са създадени следните четири дирекции: „Ковчежничество", „Анализ и контрол на риска", „Емисионно касова" и „Емисионна политика и контрол". Към подуправителя, който ръководи това управление, е създадена дирекция „Икономически изследвания и прогнози" (виж фиг. 15).

Следващият подуправител ръководи две управления: „Банково" и „Фискални услуги". Към първото са изградени три дирекции: „Банкова политика", „Статистика" и „Главно счетоводство", а към второто – две дирекции: „Депозитар на държавни и гарантирани от държавата дългове" и „Прогнози и управление на касовите потоци на държавния бюджет.

В структурата на управление „Банков надзор", ръководено от третия подуправител, са включени следните пет дирекции: „Правно обслужване и административна дейност", „Надзорна политика", „Специален надзор", „Надзорни макроанализи и стратегии" и „Надзорно наблюдение на кредитните институции".

Освен това пряко подчинени на управителя на БНБ са следните шест дирекции: „Финансова стабилност", „Правна", „Международни отношения", „Управление на човешките ресурси", „Връзки с обществеността" и „Банкова сигурност и защита на класифицираната информация".

Главният секретар на банката е отговорен за дейността на следните четири дирекции: „Обществени поръчки", „Информационни системи", „Административна" и „Стопанска".

Б. Федералната резервна система (Federal Reserve System) на САЩ има следната структура:

1. Съвет на управляващите (Board of Governors of the Federal Reserve System);
2. 12 регионални федерални резервни банки;
3. Банки, които са членове на Федералната резервна система (ФРС);
4. Депозитни учреждения, нечленуващи във федералната резервна система.

В рамките на федералната резервна система функционират следните важни органи:

1. Комитет по операциите на открития пазар (Federal Open Market Committee);
2. Федерален консултативен съвет (Federal Advisory Council);
3. Апарат на ФРС.

Съветът на управляващите се състои от седем члена, всеки от които заема своя пост в течение на 14 години. На всеки две години един от членовете на съвета, които се назначават от президента на САЩ, напуска неговия състав. Само един представител на федералните резервни банки може да стане член на съвета. Един от членовете на съвета се назначава за председател, а друг – за негов заместник. Председателят може да заема своя пост за срок от едва 4 години.

Независимостта на Федералната резервна система от изпълнителната и законодателната власт се изразява в следните три направления: 1) независим източник на доход на съвета; 2) стъпаловидни срокове на пълномощия 3) освобождаване от контрол от страна на главното управление по бюджетен контрол.

Към дванадесетте федерални резервни банки има разкрити 25 филиала. Във всеки от дванандесетте окръга банките-членове на ФРС са акционери в своята федерална резервна банка, като притежават нейни акции на стойност, равна на 3% от собствения им капитал. Те избират шест от деветте директори на тази банка. Последните се подразделят на директори от първи ранг, които представляват банковия сектор, директори от втори ранг, представляващи промишлените предприятия и директори от трети ранг, представляващи държавните органи и обществеността. Банките-членове на ФРС избират директорите от първи и втори ранг, а директорите от трети ранг се назначават от съвета на управляващите ФРС. Директорите имат

мандат от три години, като един директор от всеки ранг се избира или назначава всяка година. Съветът на управляващите ФРС избира председател на съвета на директорите и негов заместник за всяка федерална резервна банка.

В. Европейската централна банка (ЕЦБ) - заедно с националните централни банки на страните-членки на Европейския съюз формира Европейската система на централните банки (ЕСЦБ). Евросистемата включва само централните банки на страните от еврозоната. Органите за вземане на решения на ЕЦБ са Управителния съвет и Изпълнителния съвет.

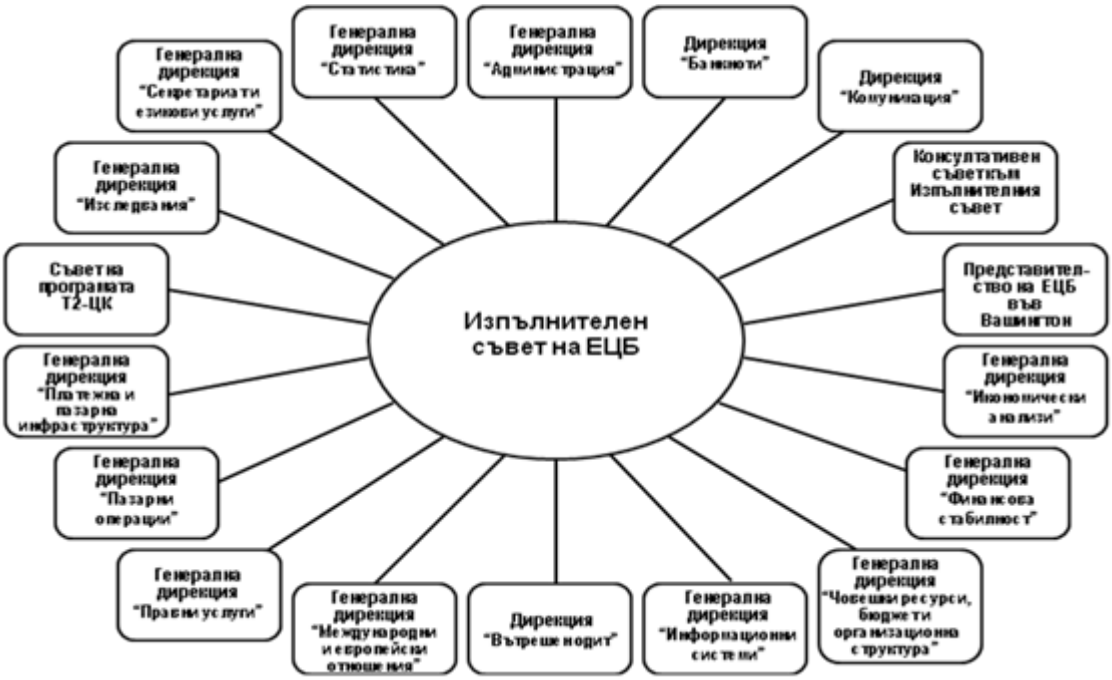
Управителният съвет - състои се от членовете на Изпълнителния съвет на ЕЦБ и от управителите на националните централни банки на страните, приели еврото. Основните му отговорности са следните:

- Да приема насоки и да взема решения за осигуряване изпълнението на задачите, възложени на Евросистемата;
- Да формулира паричната политика на еврозоната, както и решения, свързани с междинните цели на паричната политика, да определя основните лихвени проценти и да осигурява резервите на Евросистемата.

Изпълнителният съвет - включва президента и вицепрезидента на ЕЦБ, както и още четирима членове, назначени с общото съгласие на страните-членки на ЕС, приели еврото. Отговорностите му са следните:

- Да подготвя срещите на Управителния съвет;
- Да прилага паричната политика на еврозоната в съответствие с насоките и решенията на Управителния съвет и да дава необходимите указания на националните централни банки от еврозоната;
- Да упражнява определени правомощия, делегирани му от Управителния съвет, включително и такива с регулаторен характер.

Към Изпълнителния съвет функционират определени структурни звена, изградени от различни генерални дирекции, дирекции и сектори, които подпомагат неговата дейност (виж фиг. 16).



Фиг. 16 Организационна структура на Европейската централна банка

Комитети - съществена роля при подпомагането на органите за вземане на решения на ЕЦБ играят различни комитети на Евросистемата (ЕСЦБ). По искане на Управителния съвет и Изпълнителния съвет комитетите осигуряват необходимата информация в своите сфери на компетентност и подпомагат процеса на вземане на решения. Те са следните:

- Комитет за счетоводство и парични приходи;
- Комитет за банков надзор;
- Комитет за банкнотите;
- Комитет по методология за изчисляване на разходите;
- Комитет за комуникации на Евросистемата/ЕСЦБ;
- Комитет за информационни технологии;
- Комитет на вътрешните одитори;
- Комитет по международни отношения;
- Правен комитет;
- Комитет за пазарни операции;
- Комитет по парична политика;
- Комитет за платежни и сетълмент системи;
- Комитет по статистика.

Освен това са изградени и три нови спомагателни звена. Така например Бюджетният комитет подпомага дейността на Управителния съвет по въпроси, свързани с бюджета на Европейската централна банка. Конференцията за човешките ресурси е създадена с цел обмяна на опит, експертни становища и информация между централните банки в областта на управлението на човешките ресурси. Координационният комитет по информационни технологии е създаден с основна задача да координира усъвършенстването при използването на информационните технологии в рамките на Евросистемата в съответствие със заявената й мисия и с организационните й принципи, насочени към постигане на взаимодействие и извличане на печалби от ефективността на разходите посредством реализиране на икономии от мащаба.

Дейността на ЕЦБ се контролира от външен одитор, назначен да извършва одит на годишните отчети на ЕЦБ и Европейска сметна палата, която проверява ефективността на управлението на ЕЦБ. Системата за вътрешен контрол на ЕЦБ е изградена въз основата на подход, според който всяко структурно звено носи отговорност за управлението на поемания от него риск и за ефективността на своята дейност. Задачите по одита се изпълняват от Дирекция „Вътрешен одит” под прекия контрол на Изпълнителния съвет.

2.8.Други финансови институции

Факторингът е търговска операция, при която дадена фирма "продава" своите вземания (по фактури) от клиенти на трето лице в замяна на незабавно плащане, което в общия случай е по-малко от номиналната фактурирана стойност на вземанията. [6]

По своята икономическа същност факторингът е много близък до форфетирането с тази разлика, че при последното става въпрос за конкретна сделка по внос-износ (а не за цялата съвкупност от балансови вземания). В този смисъл - форфетирането е частен случай на факторинга.

Икономическият смисъл на операцията е да бъде освободен оборотният капитал на фирмата, "замразен" във вземания по неплатени фактури, и да бъде реинвестиран в текущата дейност на фирмата. Факторингът според определението в т.12 на §1 от допълнителните разпоредби на ЗКПО "е сделка, при която едно лице (фактор) купува по силата на договор за цесия еднократни или периодични парични вземания, произтичащи от доставка на стоки или предоставяне на услуги, като поема риска от събирането на тези вземания срещу заплащането на определено възнаграждение". Факторинговите сделки са предмет на дейността и на банките и небанковите финансови институции. Договорът за факторингова сделка е двустранен, възмезден и дългосрочен и съдържа елементи на договора за цесия и договора за извършване на услуга. Отношенията по факторингова сделка включват три страни:

- ✓ предприятие, което продава стоки или услуги с отсрочено плащане;

- ✓ предприятие - купувач на стоки или услуги, което е платец по сделката с предприятието продавач;
- ✓ фактор - лице (банка, небанкова институция, предприятие), което действа като агент, поемайки задължението да събере вземането от купувача платец и да го предостави на продавача.

Видове Факторинг

Открит и скрит факторинг - при открития факторинг длъжникът по сделката, в лицето на купувача е информиран за прехвърлянето на вземанията и той извършва плащането пряко към фактора. При скритията факторинг купувачът не е уведомен за фикторинговата операция и плаща дължимата сума на продавача. Съгласно сключения от него договор, продавачът получава определените суми като представител на фактора и му ги предава или влага в отделна банкова сметка на негово име.

Същински и несъщински факторинг - при същинския факторинг факторът поема риска и той купува вземанията без право на регресен иск към продавача на стоките и услугите. При несъщинския факторинг продавачът остава регресивен длъжник и е потенциално изложен на претенции от страна на фактора за изплащане на дължимите суми по вземанията.

Договорът за факторинг предвижда възнаграждение за фактора. В него се включва обичайният пазарен процент комисиона за извършване на операциите по сделката, както и сума за покриване на разходи по ползван кредит, ако с него плаща на продавача. Като елемент на възнаграждението може да се разчита и разход за застраховане на риска. Възнаграждението се договаря в абсолютна сума или в процент от стойността на сделката. Факторинговата сделка е облагаема доставка по ЗДДС. Това е регламентирано в чл.36, т.3 на закона. Облагаемата основа се определя от размера на възнаграждението по договора, а самата стойност на вземането е необлагаема, тъй като тя е обложена при сделката за покупко-продажба между продавача и купувача.

Форфетингът представлява договорено финансиране, чрез покупка на вземания от стокови доставки и услуги от специализирани финансови институции (банки или други кредитни институции). [6]

Могат да бъдат изкупени както авалирани менителници на вносители, така и открити счетоводни вземания. Обикновено вземанията са за крупни суми и се извършват в срок до 7 години. Тъй като купувачът на вземанията се отказва от претенции към продавача се изискват допълнителни гаранции. Основание за извършване на финансовата операция е договор за форфетинг, който се подписва между заинтересованите страни по сделката.

Форфетирането е метод за финансиране на дълготрайни материални активи с фиксиран лихвен процент по кредита за нови дълготрайни материални активи. Периодът е от 5 до 7 години.

Участниците във форфетирането са форфетьорът длъжникът по търговската сделка и първоначалният кредитор.

Форфетьорът е специализираната институция, която купува вземания и по този начин я осигурява финансово. Той:

- ✓ винаги купува точни вземания;
- ✓ отказва се от регрес на риска към продавача;
- ✓ поема всички рискове по вземането;
- ✓ изкупува вземането изцяло и глобално;
- ✓ изплаща незабавно еквивалента на вземането;
- ✓ удържа лихвите до деня.

Глава 3. ОСИГУРЯВАНЕ ИНФОРМАЦИОННА СИГУРНОСТ; ИНТЕРНЕТ БАНКИРАНЕ; БЕЗКОНТАКТНИ ПЛАЩАНИЯ

3.1.Определение за информационна сигурност:

Понятието информационна сигурност обикновено се разглежда в следните перспективи:

- ✓ Състояние на защитеност на информационната среда;
- ✓ Концепция за защита на програми и данни от случайно или умишлено изменение, унищожение, разгласяване или използване без разрешение;
- ✓ Процес на осигуряване защита на информационните технологии осигуряващи работата на информационните системи;
- ✓ Отсъствие на недопустим риск, свързан с изтичане на информация по технически канали, несанкционирани или непреднамерени въздействия върху данните или други ресурси на информационната система;
- ✓ Защита на информацията, това е процес насочен към достигане състояние на защитеност но информационната среда;

3.2.Цели на информационната сигурност

- ✓ Да обезопаси ценностите на системата;
- ✓ Да защити и гарантира точност и цялостност на информацията;
- ✓ Да минимизира разрушенията, получени вследствие на модифициране или разрушаване на информацията;

3.3.Изисквания към информационната сигурност

Отчет на всички събития в хода на които информацията се създава, модифицира, осигурява се достъп до нея или се разпространява;

Основни категории информационна сигурност

- ✓ Конфиденциалност (confidentiality) - достъпност на информацията само за определен кръг лица;
- ✓ Цялостност (integrity) - гаранция за съществеване на информацията в изходен вид;
- ✓ Достъпност (availability) – възможност за получаване на информация от авторизиран потребител в удобно за него време.

Второстепенни категории информационна сигурност

- ✓ Подотчетност (accountability) – осигуряване идентификация достъпа на субекта и регистрация на неговите действия;
- ✓ Достоверност (reliability) – удостоверяване съответствие с прогнозирано поведение или резултат;
- ✓ Автетичност (authenticity) — установяване идентичност на субект или ресурс с обявените.

Обхват на понятието информационна сигурност

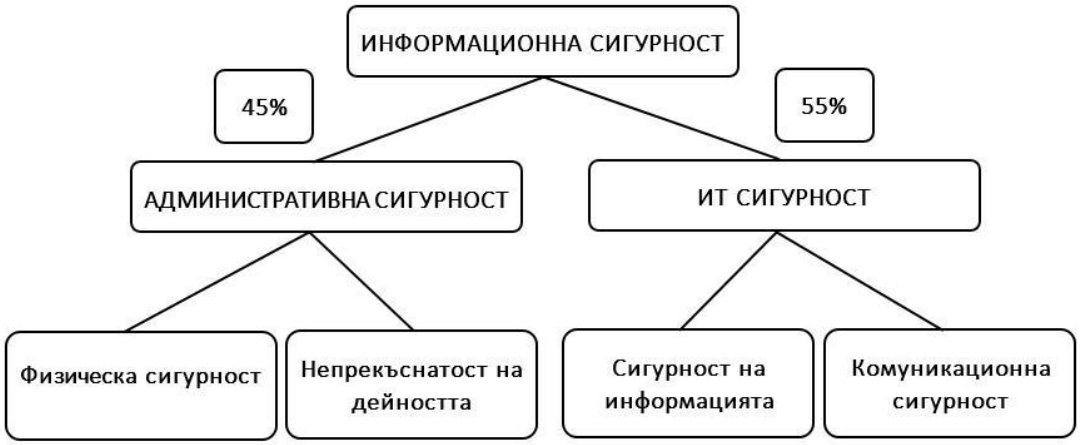
- ✓ Законодателна, нормативно-юридическа и научна база;
- ✓ Структура и задачи на органите, осигуряващи сигурност на информацията;
- ✓ Организационно-технически подходи и методи;

- ✓ Програмно-технически начини и средства за осигуряване на информационната сигурност;

Системен подход към информационната сигурност

- ✓ Взаимосвързани и развиващи се компоненти и подсистеми;
- ✓ Изграждане на вътрешна йерархия;
- ✓ Процесите се разглеждат на принципа от общото към частното;
- ✓ Дейността се осъществява чрез прилагане на конкретна стратегия;

3.4.Структура на информационна сигурност



Фиг.17 Структора на информационната сигурност

3.5.Базови характеристики на информационната сигурност

- ✓ Информационната сигурност се основава на изискванията на законите, стандартите и нормативните документи;
- ✓ Информационната сигурност се обезпечава от набор средства и дейности – организационни, програмни, апаратни;
- ✓ Средствата за защита трябва да предвиждат контрол на тяхната ефективност;
- ✓ Средствата за защита трябва да допускат оценка на тяхната ефективност;
- ✓ Средствата за защита не трябва да снижават функционалните характеристики на информационната система;

3.6.Информационната сигурност и бизнеса

- ✓ Информационна сигурност се явява част от процеса по управление на рисковете в бизнес организациите;
- ✓ Информационната сигурност е тясно свързана с всички процеси в организацията;

3.7.Нива на информационна сигурност

- ***Базово ниво на информационна сигурност***

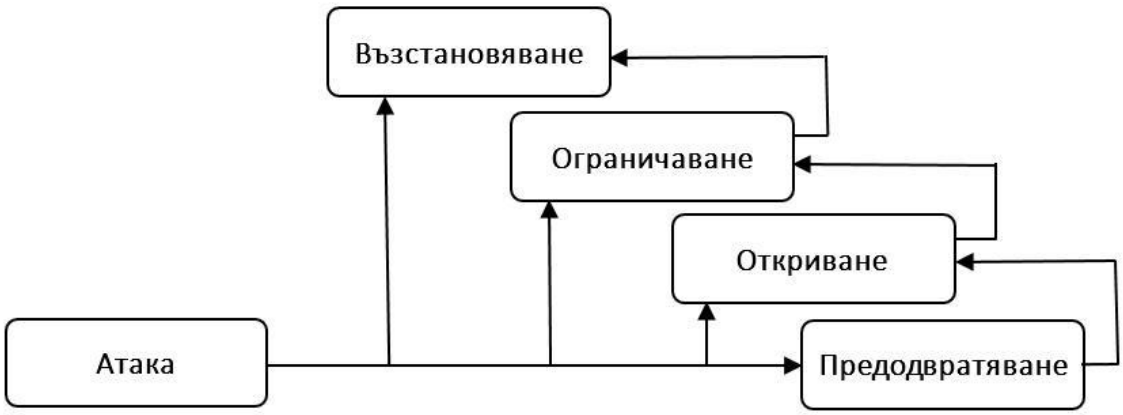
Средствата за защита трябва да се противопоставят на отделни атаки от физически лица;

- ***Средно ниво на информационна сигурност***

Средствата за защита трябва да се противопоставят на колективни атаки от лица, притежаващи ограничени възможности;

- ***Високо ниво на информационна сигурност***

Средствата за защита трябва да се противопоставят на колективни атаки на лица с потенциално неограничени възможности;



Фиг. 18 Нива на противойдействие на външна атака

3.8.Интернет сигурност

В своето ежедневие, повечето от нас използват интернет. Ние изпращаме е-мейли, разменяме съобщения, забавляваме се, купуваме и продаваме, а също така използваме и електронни банкови услуги за своите разплащания. Употребата на дигитални услуги в ежедневието, създава и възможности пред киберпрестъпниците за извършване на злонамерени действия чрез:

- ✓ Присвояване на идентичност чрез инсталиране на „шпионски софтуер" или заразяване с вирус и получаване на дистанционен достъп до лични данни
- ✓ Изпращане на подвеждащи съобщения до вашия е-мейл и приканване към действия с цел финансова измама
- ✓ Изпращане на съобщения, подканващи ви към посещение на „фалшива страница" и споделяне на ваши лични данни (e-mail phishing)
- ✓ Хакване на вашата безжична мрежа и следене на вашето онлайн поведение

Кои са най-честите заплахи в интернет?

Кражба на идентичност

Кражбата на идентичност е престъпление, при което измамник се сдобива с ключови лични данни като например дата на раждане, детайли за банкови сметки или номер на шофьорската книжка, с цел да се представи за някого другиго. Откритите лични данни, след това се използват незаконно за кандидатстване за кредит, закупуване на стоки и услуги или получаване на достъп до банкови сметки – т.е. за извършване на криминални действия от името на жертвата.

Прихващане и запаметяване на активността на клавиатурата / на легитимирането при влизане (логване)

Всичко, което пишете чрез клавиатурата на компютър, може да бъде прихванато и запаметено. Това може да се извърши чрез устройство, прикрепено към Вашия компютър, или чрез софтуер, който функционира на компютъра почти невидимо. Легитимирането при влизане (логване) често се използва от измамници за прихващане на лични данни, включително и пароли. Някои най-нови вируси дори са в състояние да инсталират такъв софтуер без да събудят подозрението на потребителя. Рискът това да Ви се случи е по-голям когато използвате компютри, споделяни от няколко потребители, например компютрите в

интернет клубове. Съвременна антивирусна програма и „защитна стена”(firewall) ще спомогнат за отстраняване на вреден софтуер преди да стане възможно да се използва.

Зловреден софтуер (малуер)

Названието „малуер”/ "malware" е съкратено от 'malicious software'. Такъв софтуер има за цел проникване в компютърната система без Ваше съгласие. Терминът обхваща различен натрапен софтуер/програми, включително вируси, „червеи”, „троянски коне” и шпионски софтуер.

Най-честите „Троянски коне” при банкирането през 2013 са:

- ✓ Threat
- ✓ Zbot +
- ✓ Gameover
- ✓ Cridex
- ✓ Shylock
- ✓ Spyeye
- ✓ Bebloh
- ✓ Mebroot
- ✓ Tilon (Tiylon)

Фишинг (Phishing)

При фишинга се изпращат писма по електронна поща до толкова адреси, с колкото измамникът успее да се сдобие. Обикновено в тези писма се твърди, че са изпратени от законна организация, например банка или търговец в интернет. Чрез писмото се изисква получателят да актуализира или да потвърди своите лични и финансови данни, включително дата на раждане, информация за легитимиране при влизане (логване), подробности за сметка, номера на кредитни карти, пин кодове и др. Писмото съдържа линк, който Ви препраща към фалшив сайт, който изглежда също като автентичния сайт на организацията (или е много подобен на него). Така измамникът прихваща лична информация като например пароли. Чрез кликване върху линк е възможно също и да изтеглите в своя компютър зловреден софтуер, който записва бъдещото използването на интернет от Вас и изпраща на измамника още повече информация. След това тази информация се използва от измамниците за достъп до банкови сметки, кредитни карти и др.

Шпионски софтуер (Spyware)

Това са програми или файлове, които може вече да са инсталирани във Вашия компютър и често се получават като скрити компоненти на „безплатни” програми. Шпионският софтуер следи използването на интернет и в по-крайните си форми може да включва прихващане на легитимирането чрез клавиатурата и виртуално наблюдение на цялата Ваша компютърна активност.

Троянски кон

Софтуер, който изглежда легитимен, но пренася нежелано приложение, например вирус или шпионски софтуер, обикновено използван от хакери, за да си осигурят незаконен достъп до компютърни системи.

Вирус

Компютърна програма, проектирана да се размножава, копирайки се в други програми, инсталирани в компютъра. Тя може да е и безвредна, но обикновено има отрицателен ефект, например забавяне на действието на Вашия компютър или увреждане на паметта и файловете. Понастоящем вирусите се разпространяват главно чрез електронната поща, чрез услуги за споделяне на файлове и чрез подвижни външни устройства като HDD, USB памет, CD/DVD.

Фалшиви предупреждения по електронна поща за вирус

Много от предупрежденията по електронна поща за вируси са лъжливи и имат за цел просто да предизвикат безпокойство и да разстроят различни бизнеси. Такива

предупреждения може да са и автентични, така че не гледайте на тях несериозно, но винаги проверявайте какъв е случая, като посетите антивирусен сайт като например McAfee, Sophos или Symantec преди да предприемете някакви действия или да ги препратите на приятели и колеги.

Червеи

Това е зловредна програма, която се размножава, докато запълни цялото пространство за съхранение в компютърно устройство или мрежа. При размножаването си червеите могат да изразходват компютърно време, място и скорост, а зловредното намерение е да се забави работата на цели уеб сървъри или те за бъдат блокирани и да се разстрои използването на интернет.

3.9.Как да се защитим в интернет пространството. Основни правила.

Има няколко основни правила, които осигуряват най-голяма защита в мрежата при най-малко усилия. Това не са всички мерки, които можете да вземете, но са едно отлично начало – и важат еднакво както за собственици на бизнес, така и за частни лица.

- ✓ Защитете паролата си;
- ✓ Излезте от системата след приключване;
- ✓ Деактивирайте функциите "Автоматично попълване" и "Запаметяване на пароли на браузъра си;
- ✓ Защитете компютъра си;
- ✓ Проверявайте автентичността на сайта, на който сте;
- ✓ Блокирайте спама;
- ✓ Защитете своята WiFi мрежа;
- ✓ Пазете данните си;

Защитете паролата си

Вашата парола осигурява важна защита, за да е сигурно, че можете да изпълнявате онлайн дейности в пълна безопасност. Обаче, за да осигурява оптимална защита, една парола трябва да съответства на най-добрите практики за сложност, посочени по-долу. Изберете сложна парола: лесна за помнене, но трудна за отгатване – т.е. поне 10 символа, включително малки и главни латински букви, цифри и специални символи (#, @, $, % …). Изборът на „силна” парола е защита против кражба на идентичност. Вашата парола не трябва да бъде тривиална (не повтаряйте едни и същи цифри или серии от цифри) и не трябва да е лесно за други лица да я предположат (напр. рождената Ви дата). Избирането на определени букви от даден текст/изречение като например любим стих или думи на литературен герой, може да е добър вариант.

Използване на паролата: въвеждайте Вашия код единствено в надеждната страница за вход на Вашата банка онлайн. Променяйте паролата си редовно и не я повтаряйте.

Никога не разкривайте паролата си на никого. Вашата банка, както и всяка сериозна и надеждна институция никога няма да Ви пита за Вашата парола.

След като свършите с разглеждането на сметката си, излезте от системата

Когато влезете в услугата за онлайн банкиране, се открива сесия за разглеждане на Вашата сметка. Докато тази сесия е активна, можете да навигирате от страница на страница и да извършвате определени операции, без да се налага отново да се идентифицирате. Когато тази функция е активна, тя позволява на всеки, който използва Вашия компютър, да разглежда Вашата сметка и да извършва операции без Ваше знание. Много важно е след като свършите с разглеждането на Вашите сметки да излезете от системата, използвайки бутона „изход”. Не е достатъчно просто да затворите страницата или браузъра. Помнете, че банката не може да отхвърли транзакция, изпълнена по време на сесия, открита от Ваше име.

Деактивирайте функциите „Автоматично Попълване" и „Запомняне на пароли" във Вашия браузър

Повечето уеб браузъри предлагат да запаметят като настройки по подразбиране потребителските имена и пароли, които използвате във форми за вход, включително данните за вход във Вашите профили в социални мрежи, акаунти за електронна поща и онлайн банкиране. Функциите „автоматично довършване" (AutoComplete) и „запомни моята парола" (Remember my password) Ви дават възможност да влезете в акаунта си по-късно без да се налага отново да въвеждате потребителското си име. Макар това да е удобно, функциите„автоматично довършване" и „запомни моята парола" могат да помогнат на лице, използващо Вашия компютър, да влезе във Вашия акаунт без Ваше знание.

Защитете Вашия компютър

Преди да разглеждате уебстраници в интернет би трябвало да защитите компютъра си от потенциални злонамерени атаки чрез прилагане на лесни мерки като следните:

Уверете се, че имате най-новите версии на програмите и лицензиран софтуер: от време на време се откриват недостатъци в програмите, инсталирани на Вашия компютър. Тези недостатъци могат да бъдат използвани от създателите на вируси и от хакери, за да получат дистанционен достъп до компютрите. Лицензираните издатели понякога пускат обновяващи пакети за програми, за да коригират тези слабости. За да проверите за такива пакети и актуализации, трябва да посетите уебсайта на издателя, обикновено техния раздел „Изтегляне", или да конфигурирате компютъра си за автоматично изтегляне на всички обновяващи пакети и най-новите актуализирани програми при влизането Ви в интернет. Обикновено най-сигурни са най-новите версии от групата на операционна система (като Microsoft Windows) или браузър (като Internet Explorer, Firefox и др.). Потребителите на Microsoft могат да посетят следния адрес: http://windowsupdate.microsoft.com , който може автоматично да провери какво е необходимо за Вашата операционна система и Вашия браузър, и след това да го изтегли по Ваше искане.

Инсталирайте лицензирани антивирусни програми: би трябвало да инсталирате антивирусна програма на компютъра си, за предпочитане лицензирана, тъй като това ще Ви гарантира поддръжка при заразяване с вирус и редовно осъвременяване срещу най-новите опасности. Такъв софтуер защитава Вашето легитимиране и блокира инсталирането на зловреден софтуер на компютъра Ви. Антивирусните програми освен това проверяват надеждността на файловете, които изтегляте от интернет, копирате в компютъра си от външни устройства или получавате по електронна поща. Най-важното за Вашата антивирусна програма е постоянно да се актуализира.

Използвайте защитна стена: личната защитна стена е друга възможност, която Ви помага да защитите компютъра си и неговото съдържание от външни лица в интернет. Когато бъде инсталирана и правилно конфигурирана, тя спира неоторизирания трафик от и към Вашия компютър. Съществуват много ефективни програми, измежду които може да изберете.

Най-разпространените търговски примери включват Windows Firewall и Check Point Zone Alarm (безплатни), лична защитна стена McAfee и лична защитна стена Norton. Всички операционни системи са придружени с опция за такава лична защитна стена и е само въпрос на усилие за проста конфигурация от Ваша страна, което прави безопасно разглеждането от Вас на страници в интернет след това.

Използвайте програма против шпионски софтуер: Наличните понастоящем програми против шпионски софтуер включват AdAware, Microsoft Defender (безплатно), Spyware Blaster, Spy Sweeper и Sunbelt Software Counter Spy. При такива програми също е необходимо да посетите оригиналния уебсайт, тъй като съществуват много фалшиви продукти, за които се твърди, че защитават Вашия компютър, но те могат всъщност да го заразят с вируси.

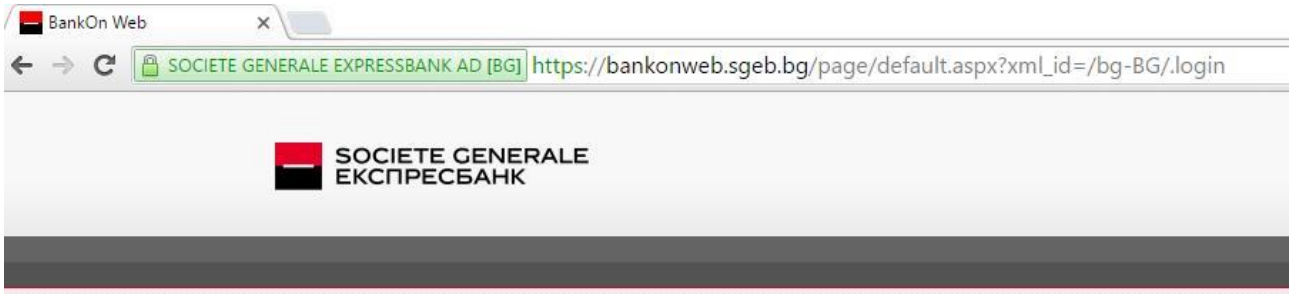
Проверявайте надеждността на сайта, който посещавате

Независимо дали сте влезли в сайт за електронно банкиране или електронна търговия, важно е преди да въведете данните си за легитимиране или да извършите някакви транзакции, да се уверите, че сайтът е официален и сигурен, като направите следното:

Проверете URL адреса на сайта в полето за адреса: URL адресът е уникален идентификатор за уеб страницата, на която се намирате, и се вижда в полето за адреса във Вашия браузър. Проверявайки внимателно този адрес ще можете да разберете дали сайтът, на който се намирате, е подправен, тъй като такъв адрес неизбежно се различава от този на официалния сайт (например www.sgeb.bg)

Проверете префикса на адреса: Всички официални сайтове за интернет банкиране или електронна търговия обикновено използват защитен протокол за комуникация със своите клиенти. Ако се намирате на защитен сайт, URL адресът ще се предхожда от "https" (вместо"http")

Проверете сертификата за сигурност: Сертификатът се използва за гарантиране, че институционалният уебсайт, в случая зя пример е използвана Societe Generale Expressbank и нейният сайт за електронно банкиране са легитимните сайтове. Това се потвърждава също и чрез сертификат VeriSign Certificate, който показва в зелен цвят "SOCIETE GENERALE EXPRESSBANK AD" на Вашия браузър и Ви защитава от фишинг атаки.



Фиг.19 Пример за интернет сертификат за сигурност

Блокирайте спам съобщения по електронна поща

Нежеланите съобщения (спам) могат да се използват за начало на фишинг атаки, като Ви приканват да кликнете върху линкове, които след това прехвърлят зловреден софтуер на Вашия компютър или Ви насочват към фалшив уебсайт. Ако получите писмо по електронна поща от неразпознат източник, следва да го изтриете без да го отваряте. Би трябвало освен това да можете да активирате филтър за спам, който автоматично насочва всички такива писма към отделна папка за входящи съобщения. Изтриването на нежелания спам, без да го четете, също ще Ви предпази от повечето писма, които имат за цел фишинг. Никоя банка никога не изпраща на клиентите си непоискани писма по електронна поща, съдържащи линк към която и да е от страниците за вход в системата. Ако получите такова писмо, не го отваряйте и не изтегляйте прикрепени файлове, а се обадете в банката, за да проверите за какво става дума и да получите помощ.

Защитете своята WiFi мрежа (безжична мрежа)

Безжичната мрежа Ви дава възможност да свързвате компютъра си с интернет без да се налага да използвате кабел. Тя обикновено съдържа безжичен рутер, който използва радиосигнали, за да предава данни към компютри в рамките на мрежата. Безжичните рутери се доставят с предварителни настройки, които са много несигурни, така че дават възможност много потребители да се свързват към тях едновременно, и в повечето случаи не са защитени дори с парола – това означава също, че други лица могат да следят трафика и да влязат във Вашия интернет акаунт доста лесно. Поради тази причина следва винаги да направите справка в указанието или в онлайн наръчник, за да разберете как по-безопасно да се свързвате чрез Вашата безжична мрежа – обикновено като я защитите чрез парола.

Погрижете се за данните извън мрежата

Преглеждайте извлеченията от Вашите банкови сметки и кредитни карти за наличие на необичайни транзакции или тегления и незабавно уведомете банката ако подозирате, че има някакви несъответствия.

Уведомявайте за промените във Вашите лични данни (като промяна на адрес, телефонен номер, адрес на електронна поща и др.)

Пазете Вашите писмени документи по надежден начин. Съхранявайте банковите си документи на сигурно място. Избягвайте да ги изпращате на трети страни по незащитен начин (например по електронна поща; оставяне в разпечатан вид на публично място, и т.н.). Винаги ги унищожавайте чрез шредер когато вече не са необходими.

Ако възнамерявате да анулирате банкова или кредитна карта (или ако изтече нейният срок на валидност), върнете я в банката, където ще бъде перфорирана през номера на сметката и магнитната лента.

Защитете мобилното си устройство

Все по-широкото използване на смартфони и разработването на повече банкови услуги за такива устройства водят до възникването на нови рискове за сигурността. Смартфоните често биват оприличавани на мобилни телефони, но на практика те са миникомпютри, които могат да се използват също и за телефонни обаждания. Затова мерките за сигурност, които се отнасят за компютър (виж по-горе), са валидни и за смартфон.

Смартфоните обаче изискват и допълнителни защитни мерки:

Защитете Вашия телефон с (нетривиална) парола и задайте автоматично заключване на екрана когато не се използва.

- ✓ Уверете се, че използвате всички актуализирани средства, препоръчани от Вашия системен доставчик;
- ✓ Изтегляйте приложения само от официални магазини за приложения (например Apple Store, Google Play Store). В противен случай рискувате да инсталирате в смартфона си зловредни приложения;
- ✓ Никога не отключвайте операционната система на вашия смартфон (напр. чрез jailbreak, rooting), тъй като това Ви излага на повече рискове;
- ✓ Не съхранявайте в смартфона си некриптирани поверителни данни;
- ✓ Инсталирайте антивирусен софтуер и редовно го актуализирайте;

Защитете своята организация

Вируси, спам, фишинг, хакери, кражби и измами с кредитни карти – това са само някои от проблемите със сигурността, пред които е изправен бизнесът днес. За да научим как може да засилим сигурността си и да защитим бизнеса си от финансови загуби, ще разгледаме по-долу описаните рискове и начини за защита. [9]

- ✓ Оценете рисковете;
- ✓ Обучавайте служителите си;
- ✓ Защитете системите си;
- ✓ Разговаряйте с клиентите си;
- ✓ Докладвайте за злоупотреби;

Оценка на риска

Правите оценка на риска на Вашата компютърна среда периодично. Бизнес потребителите на онлайн банкиране следва да извършват периодична оценка на риска и оценка на контрола на своята компютърна мрежова среда. Това трябва да се прави минимум веднъж годишно.

Направете списък на начините, по които фирмата събира, използва и съхранява клиентска и бизнес информация. Документирайте как служителите получават достъп до клиентска и бизнес информация, включително дистанционно.

Установете по какъв начин информацията може да бъде изложена на риск, откраднатa или използвана. Включете оценка на риска за клиентска информация, както и за поверителна

бизнес информация, включително интелектуален капитал. Документирайте начините за контрол, въведени за защита на Вашата компютърна и мрежова среда.

Определете необходимите допълнителни средства за контрол. За всяко от тях проверете дали представлява одобрен проект и ако е така – кога ще бъде реализиран; ако не е одобрен – какво е неговото състояние.

Отбележете евентуални „инциденти, свързани със сигурността", които са станали след последната оценка на риска. Изяснете какво се е случило, какво е било въздействието, в кои от съществуващите средства за контрол е имало пробив – ако е имало такъв, и/или какви средства за контрол да бъдат въведени, за да се избегнат такива събития в бъдеще.

Образовайте своите служители

Колкото и да е защитена Вашата техническа среда, едно погрешно кликване с мишката от даден потребител може да изложи на сериозна опасност Вашия бизнес. Вашите служители могат да бъдат най-силното или най-слабото звено в плана Ви за сигурност. Следвайте нашите полезни съвети, за да помогнете на служителите си да станат Ваши най-силни съюзници по отношение на сигурността.

Можете да инсталирате защитни стени на всеки компютър, да актуализирате софтуера си и да създадете резервни копия на Вашите данни, но ако служителите Ви не следват добри практики за сигурност, бизнесът Ви ще е уязвим за широк кръг опасности. Помогнете на служителите да разберат защо имате политика за сигурност и защо те трябва да я приемат сериозно. Сигурността на Вашия бизнес е в техните ръце.

Защитете Вашите системи

Ако направите сигурността свой приоритет, това може да Ви помогне да избегнете принудително бездействие и разстройване на дейността. За да защитите компютрите си от интернет опасности и загуба на данни, следвайте най-добрите практики като например ISO 27001, NIST, NSA и др. Дори да нямате ресурсите на голям бизнес със специален IT отдел, компанията Ви е изложена на такива опасности. Следването на добри практики във връзка със сигурността може да намали рисковете и да сведе до минимум бъдещи щети.

Разговаряйте с Вашите клиенти

Вашата политика за поверителност засяга всички. Уведомете клиентите си как да защитят данните си. Изграждането на взаимно доверие с Вашите клиенти е полезно за бизнеса Ви. В действителност едно неотдавнашно проучване показа, че повечето потребители биха препоръчали даден бизнес ,ако са уверени, че той прилага своята политика за сигурност и защита на личните данни. Вашите клиенти желаят да знаят как ще се използва и как ще бъде защитена личната им информация. Ваша отговорност е да ги уведомите за това.

Съобщавайте за злоупотреби

Следвайте тези важни стъпки, за да спомогнете за ограничаване на щетите и разстройването на Вашия бизнес. Жизненоважно е да имате подходящ план за справяне с инциденти, свързани със сигурността, така че да можете да предприемете незабавни стъпки за ограничаване на щетите и разстройването на дейността Ви, и съответно да уведомите засегнатите страни. Част от плана Ви би трябвало да включва създаване на резервни копия на важни файлове и програми. Това ще Ви спести време и пари и ще Ви позволи да не прекъсвате работа докато решите проблема.

3.10. Интернет банкиране / Електронно банкиране / On line banking

Интернет банкирането (още "електронно банкиране") е услуга, която всички банки предлагат. С него може да се извършват някои действия виртуално, без клиентите лично да ходят до офиса на банката. Според политиката на банката, е-банкирането може да включва само някои елементарни услуги (по-безопасно), или пък да включва голяма част от услугите предлагани от банката.

Он лайн банкирането е електронна система за разплащане, която позволява на клиентити на различни финансови институции да извършват различни финансови транзакции като ежедневни разплащания по банков път, виртуално банкиране, кредитиране и др. Он лайн банкирането също така е познато като Интернет Банкиране, е-банкиране, виртуално банкиране и др.

За да получи достъп до интернет банкирането, всеки клиент имащ интерент достъп първо трябва да се регистрира за съотвеното обслужване и да зададе лична парола за достъп. Паролата за електронно банкиране през интернет обикновенно е различна от тази за банкиране през телефон.

Интеренет банкирането може да се представи най-общо в два варианта:

- Само за справка;
- Справка и реално осъществяване на определени банкови операции;

При вариант едно клиента реално не може да извършна никакви операции освен да следи движението по сметките си (тегления, внасяния, дата, контрагент еветнуално лихви или банкови такси). Реално това не може да се определени точно като интернет банкиране, тъй като нали;це не са реални операции извършвани от клиента ползвател. Той може само и единствено да извърши справка по движението на сметките си. От друга страна това е може би най-безопасния вариант при интернет банкиране. Дори някой да успее за се добере до потребителското име и парола на съответния ползвател, не би могъл да извърши нищо, тъй като налице не са никакви реални услуги свързани с прехвърляне на суми или плащания.

При втория вариант с реални банкови операции, като прехвърляне на пари и плащания потребителят има пълен или частичен пакет от услуги, в зависимост от това какво е избрал и какви са условията на съответната банка. Този вариант безспорно е по добър от първия, давайки соледин набор от услуги като прехвърляне по сметки, плащания към бюджета, насрочване на бъдещи плащания по предвалително подготвен формуляр, а в някои сучаи покупка на валута и ценни книжа. Но също така при този метод и рисковете са значително по големи тъй като нарлице е реална възвожност при изтичане на информация като потребителско име и парола, да се стигне до кражба или източване на сметките на потребителя.

Банките също са помислили за тези рискове и затова предлагат различни мерки за сигурност при интерент банкиране.

3.11.Предимства и недостатъци на онлайн банкирането

В наши дни онлайн банкирането се смята за идеалния метод за дистанционно управление на парите ни. Само с няколко клика можем да отменим широк кръг от ежедневните си платежни задачи – да направим изгодни електронни покупки, да платим някои неотложни сметки или да извършим обикновена справка.

Като всеки нов метод за синтезиране и улесняване на битовите ни задължения, опиращ се на неограничените възможности на интернет, и този има две страни. Експерти смятат, че въпреки удобството и ефикасността на електронното банкиране, сляпото доверие в него е немислимо, тъй като сигурността на финансите ни винаги остава под въпрос.

- ***Предимства***

Цена

Може би най-съществоното предимство на електронното банкиране е, че чрез него можем да спестим една малка част от средствата си заради преференциите при таксуването на транзакциите. По правило всяка онлайн услуга е по-евтина. Ако например един превод в клон на банката струва един лев, същата електронна услуга е, да кажем, 70-80 стотинки.

Многократното извършване на периодични преводи може да сумира и по-съществено спестяване, смятат от своя страна немските журналисти. Те допълват, че няколко посещения на банката по-малко отменят и някои транспортни разходи.

Удобство

Лесно можем да се досетим, че интернет услугата е много удобна за потребителите. Чрез нея се пренебрегва посещаването на банков клон или банкомат. Вместо да чакаме на досадни опашки и да попълваме ръчно серия от формуляри, можем с минимум усилия да отметнем набелязаната задача. При това – независимо къде се намираме.

Удобството важи най-вече за периодичните преводи, които правим. Можем да си позволим да използваме шаблонни съобщения („макети"), като само сменяме датата и часа им.

Спестява време и нерви

Освен обективната бързина на услугата, време ни спестява и пренебрегването на нуждата да ходим до банков клон всеки път, щом искаме да извършим определена транзакция.

В допълнение, избягваме въпросните опашки и сякаш безкрайни „бюрократщини", които, освен време, често ни костват и много нерви.

Денонощна услуга

Това е предимството, върху което акцентират и банките, и съветите на порталите. Най-вече, защото времевите ограничения, обусловени от фиксираното работно време на банковите клонове, често създават проблеми. Посредством банкомат можем да преодолеем тези ограничения, само ако става въпрос за теглене на пари или отделни справки.

Електронното банкиране осигурява работен цикъл, както и нареждане на трансфери в реално време. С други думи – независимо по кое време на денонощието въведете промяна в статуса на сметката си, тя се отразява веднага.

Преференции

За да популяризират модерния метод и да се справят с конкуренцията, все повече банки предлагат определени промоционални услуги за клиентите, избрали именно онлайн банкирането.

- ***Недостатъци***

Няма доказателство, че транзакцията е извършена успешно!

Да, ние сме направили, каквото се изисква от нас, за да дадем ход на желаната операция. Получили сме и потвърждение от системата. Нищо обаче не ни гарантира, че транзакцията е извършена не само виртуално, но и реално.

Липса на междуличностен контакт

Според проучванията на немските портали, голяма част от клиентите държат на контакта „очи в очи" с банковия служител, който се оказва излишен при електронното банкиране.

Докато някои смятат това за старомодно, други ценят възможността да получат от банката експертен съвет за финансите, които са й поверили, в частност - за операцията, която смятат да извършат. Освен това можем веднага да получим отговори и разяснения при възникнали въпроси. Това важи най-вече за извършването на по-сложни операции (например – издаването на ценни книжа), за успеха на които е необходимо да сме запознати с всички рискове.

От друга страна, за част от клиентите собственоръчното управление на сметката не спестява време. Точно обратното – ако не сме достатъчно "грамотни" в електронната система на банката или просто предпочитаме някой друг да се занимае с това, лавирането в изскачащите прозорци се превръща в досадно лутане из интернет пространството. Поне така се възприема от някои потребители.

Вируси и сривове в системата

Основно това е риска от атаки на т. нар. "троянски коне" като единствения по-съществен недостатък на услугата. Всички аналогични вируси, както и вероятността от срив в системата на банката в момента, в който оперираме със сметката си, немските портали причисляват към „неприятните изненади“, които можем да очакваме винаги, когато сърфираме.

"Фишинг" атаки

В действителност най-сериозната опасност, която ни "дебне", докато боравим дистанционно с финансите си, са именно "фишинг" (phishing) атаките от съответните "фишинг" сайтове.

Интернет страниците от този тип служат за кражба на лична информация, по-специално на данните от сметката ни. В повечето случаи авторите на "фишинг" сайтовете ги проектират така, че да изискват от нас собственоръчно да въведем данните си в определено поле. Целта е да се заблудим, че това поле е част от електронната система на банката.

Какво прави банката, за да ни защити?

За да запази доверието на клиентите си – не само що се отнася до електронната услуга, но и като цяло за поверяването на финансите си – банката се стреми да сведе рисковете до минимум.

Преди всичко разбира се тя използва подходящ софтуер с подсилена защита, за да предпази себе си и потребителите си от „злонамерен“ софтуер.

Електронен подпис

Електронният подпис е най-новото въведение за електронна сигурност. С помощта на тази технология използваната система разпознава само един потребител, който удостоверява самоличността си със създадения от него уникален подпис.

За да бъде подписан един електронен документ с универсален електронен подпис, клиентът трябва да притежава удостоверение за универсален електронен подпис, технически носители (смарт карта и карточетец) и специален софтуер за управление на карти и за работа с електронни документи.

Уникална парола

Методът „уникална парола“ всъщност представлява списък от определен брой различни пароли, които банковият служител предоставя на клиента лично. Целта е потребителят да въвежда различна парола при всеки достъп до системата, а банката да я разпознава и да го индентифицира.

Генератори за пароли

Много банки си служат с програми за генериране на пароли. При всяко влизане те използват метод, подобен на своеобразен шифър, с помощта на който ни измислят сигурна парола, базирана на личните ни данни.

SMS за всяка извършена транзакция

Този тип услуга е пригодена най-вече, за да ни предпази от риска от вируси в системата и от „фишинг“ атаки. Така получаваме информация за всяка извършена транзакция от сметката ни и имаме възможност да разберем веднага, ако някой неправомерно борави с финансите ни. При някои банки изпращането на SMS е безплатна услуга, при други съобщението се таксува.

3.12.Практическа работа при интернет банкирането; Модули

При вход в Интернет банкирането на повечето банкови системи, потребителят има достъп до следното меню:

1. Справки
2. Операции

3. Депозити
4. Настройки
5. Поща
6. Информация

На екран се появява и следната допълнителна информация:

- Състояние по сметките, регистрирани за интернет достъп със следната информация: вид, номер, валута и салдо за всяка сметка. Чрез кликване върху номер на сметка, Потребителят може да види движението и извлеченията по сметката за зададен от него период;
- Панел Операции с възможност за бърз достъп до документите, които могат да бъдат инициирани през Интернет банкирането. Чрез кликване върху даден документ, на екрана незабавно се визуализира съответния документ;
- Панел Депозити с възможност за бърз достъп до документите, които могат да бъдат инициирани през Интернет банкирането за работа с депозитните продукти на Банката;
- Информация за получени и непрочетени съобщения от Банката;
- Информация за името на Потребителя и Клиента, срока на валидност на достъпа му до Интернет банкирането и възможност за бърз достъп до регистрационните данни на Клиента;
- Валутните курсове за деня;
- Валутен калкулатор;
- Указания и Общи Условия за ползване на Интернет банкирането на Банката;
- Информация за Банката и контакти;

- **Модул Справки**

При избор на модул Справки, се визуализират сметките, регистрирани за интернет достъп със следната информация: вид, номер, валута, салдо, натрупани дебитни и кредитни обороти за текущата година, дата на последната промяна в салдото за всяка сметка. За депозитните сметки има и допълнителна информация за срока, падежа, лихвения процент и натрупаната към момента лихва по съответния депозит.

Чрез кликване върху номера на сметка, Потребителят може да види движението и извлеченията по сметката за зададен от него период.

При избор на Движение по сметка за определен период се визуализира датата, референцията, сумата и основанието за всяка операция. Ако съответната операция е инициирана през Интернет банкирането на Банката, същата може да се види чрез кликване върху бутон Покажи в колона Действие. В справката за движение по сметка, Потребителят може да зададе филтър, за да види само дебитите (задълженията) или само кредитите (постъпленията) по сметката. Движението по сметка може да бъде извлечено в екселски формат чрез натискане на бутон Excel след визуализирането на движенията за избрания период на екрана с бутон Покажи.

При избор на Извлечение по сметка за определен период се визуализират датите, на които е имало някакви операции по сметката и чрез натискане на бутон Покажи може да се вижда и/или разпечатва извлечението от сметката за съответната дата.

- **Модул Операции**

Функционалност

При избор на модул Операции, системата предоставя възможност да се извършват следните действия, които се визуализират във вертикалното меню в ляво:

1/ Избор на операция:
- Левови преводи
- Валутни преводи
- Покупко-продажба на валута

2/ За изпълнение

3/ Изпратени – информация за изпратени към Банката операции и техния статус

4/ Картотека с данни за контрагентите на Клиента

5/ Импорт на файлове

При избор на Левови Операции се появяват следните документи, които могат да бъдат инициирани от Клиента:

- Левов превод;
- Превод към бюджета;
- Превод към бюджета (многоредов);
- Искане за инкасо;
- Декларация за платени осигуровки;

При избор на Валутни преводи се появява документът за иницииране на валутен превод в страната и чужбина. Валутните преводи се изпълняват със стандартен вальор от два работни дни. Може да се нареди и превод с вальор същия или следващия работен ден с предварително съгласие на Банката и при по-висока комисиона, определена в Тарифата за таксите и комисионите на Банката. Документът за валутен превод се попълва на латиница.

При избор на Покупко-продажба на валута се появява документът за обмяна на валута. При покупко-продажба на сума над 10,000 евро или щатски долара, може да се договори преференциален курс по телефон, който курс се въвежда в документа за покупко-продажба на валута.

При кликване върху съответния документ се появява формата, която следва да се попълни от Клиента за иницииране на съответната операция. Под всяка форма има възможност да се избере едно от следните действия чрез натискане на бутони: Запази, Потвърди, Изпълни, Отпечатай, Запази в картотека.

При натискане на бутон Запази, документът се премества в секция За изпълнение, откъдето Потребителят може да го редактира, потвърди или изпрати към Банката за обработка.

При натискане на бутон Потвърди, документът се премества в секция За изпълнение, откъдето Потребителят може да го изпрати към Банката за обработка.

При натискане на бутон Изпълни, системата ще поиска въвеждане на поредния неизползван ТАН от активния списък с ТАН-ове на Потребителя, за да изпрати документа към Банката за обработка и запазва същия в секция Изпратени, откъдето Потребителят може да проследи статуса на обработка на документа (изпратен, осчетоводен, върнат).

При натискане на бутон Отпечатай, документът може да се отпечата. Тази опция е активна само за документите в секция Изпратени.

При натискане на бутон Запази в картотека, информацията за контрагента (име, банкова сметка, обслужваща банка) се запазва в секция Картотека, откъдето в последствие може автоматично да бъде изтегляна при нареждане на превод в полза на същия контрагент.

- **Секция Импорт позволява:**
  - приемане на платежни документи от файл в определен формат (в секция Импорт е приложено описание на формата на файла)
  - изпращане на приетите от файла платежни нареждания

Изпращането на приетите платежни документи се извършва от секция Импорт, За Изпълнение. Въведените документи не могат да се редактират. От секция Импорт, Изпратени може да се проследи статуса на изпратените документи.

Обработка на документ в Интернет Банкирането:

А. Иницииране

Клиентът може да инициира нареждания чрез Интернет банкирането непрекъснато – 24 (двадесет и четири) часа в денонощието. Часът на приемане на всяко нареждане в банката се регистрира и този час се приема за верен при евентуално възникнал спор между страните.

Нарежданията се считат за валидни, ако са придружени от всички необходими документи, в случай че такива се изискват съгласно законовата уредба на Република България и/или Общите условия на съответната банкова организация.

В случай, че сумата на отделно нареждане надвишава равностойността на 30,000 лева и клиентът не е освободен от подаване на декларация за произход на средства съгласно ЗМИП и ППЗМИП, то той следва да попълни полето на документа за произхода на средствата при иницииране на нареждането.

При нареждане на левов превод, свързан с изплащането на трудово възнаграждение, включително и авансовото им изплащане, клиентът трябва предварително да попълни Декларация за платени осигуровки по Кодекса за задължително обществено осигуряване.

Б. Редакция. Потвърждаване. Копиране. Изтриване. Запазване в картотека.

При избор на секция За изпълнение, на екран се визуализират чакащите за изпращане към Банката документи с информация за всеки документ (дата на иницииране, име на получателя, сметка на получателя, BIC, сума на операцията, тип документ, статус) и възможност за: 1/ селектиране на период, през който документите са запазени, потвърдени; 2/ селектиране на документи от един тип (пример: само валутни преводи или само бюджетни и т.н.); 3/ селектиране на документи по име на получател, сметка на получател, БАЕ или сума.

Броят документи, които се визуализират на екрана се определя от самия Потребител в долния ляв ъгъл на таблицата с документите, като по подразбиране се визуализират 10 документа.

В. Изпращане на документи към Банката.

Изпращането на документ към Банката се извършва от секция За изпълнение чрез маркиране на документите, които следва да бъдат изпратени към Банката, натискане на бутон Изпрати и въвеждане на TAH (транзакционен авторизационен номер). С един TAH могат да се изпратят пакетно максимум до 100 документа /нареждания/, които се визуализират на един екран. Броят документи, които се визуализират на екрана се определя от самия Потребител в долния ляв ъгъл на таблицата с документите, като по подразбиране се визуализират 10 документа.

В случай, че Потребителят желае наведнъж да изпрати всички чакащи документи, независимо от бройката, кликва Избери всички;

В случай на допусната грешка в някой от документите, изпратени в пакет, системата връща целия файл, като показва документа за корекция и характера на допуснатата грешка. В този случай използваният при първоначалното изпращане TAH не се счита за използван. Потребителят следва да маркира верните документи и да ги изпрати отново в Банката, като може да използува TAH-а от първоначалното изпращане на пакета.

При изпращане на нареждания за суми, превишаващи разполагаемостта по клиентската сметка към момента на получаването им в Банката, системата ги връща. Това не важи единствено в случаите на пакетно изпращане на автоматично обработвани от Банката нареждания, при които изпълнението на едно или няколко нареждания от пакета зависят от изпълнението на други нареждания от пакета.

При изпращане на нареждания с неправилно попълнени данни или нареждания, превишаващи лимита на лицето, което ги е подписало, системата автоматично връща документите, като изписва код, показващ причината за връщане.

Всички документи, изпратени към Банката чрез системата Интернет банкиране, се съхраняват в секция Изпратени, от където могат да се разглеждат, копират и отпечатват. При избор на тази секция, на екран се визуализират всички изпратени към Банката документи с информация за: дата на документа, име на получателя, сметка на получателя, BIC, сума на операцията, референция, тип документ, статус) и възможност за: 1/ селектиране на период, през който документите са изпратени; 2/ селектиране на документи от един тип (пример: само валутни преводи или само бюджетни и т.н.); 3/ селектиране на документи по име на получател, сметка на получател, БАЕ или сума. Разглеждането на изпратен документ става чрез кликване върху името на получателя на съответния документ. Отпечатването на изпратен документ става чрез влизане в самия документ с кликване върху името на получателя и натискане на бутон Отпечатай. Копирането става чрез маркиране на документа, който следва да се копира и натискане на бутон Копирай избраните, което копира документа в секция За изпълнение, откъдето може да се редактира, запази, потвърди и/или повторно изпрати.

Г. Статуси на обработка

В зависимост от етапа на обработка на всеки документ, статусите на документите могат да бъдат:

- "Записан" – документът е въведен в системата, но не е изпратен към Банката. Документите с този статус са оцветени в жълто.
- "Потвърден" - документът е потвърден и е готов да бъде изпратен към Банката. Документите с този статус са оцветени в синьо.
- „Повторно потвърден" - документът е повторно потвърден (когато това се изисква от зададените права на потребителя) и е готов да бъде изпратен към Банката.
- "Изпратен" - документът е изпратен към Банката, но все още не е обработен от Банката. Документите с този статус са оцветени в жълто.
- "Осчетоводен" - документът е обработен от Банката, т.е. инструкциите на клиента са изпълнени и сметката му е задължена. Документите с този статус са оцветени в зелено.
- "Върнат" - документът е отхвърлен от Банката и няма да бъде изпълнен. Отхвърлянето е придружено с описание на причината за отхвърляне. Документите с този статус са оцветени в червено. Върнатите или отхвърлените от Банката документи се показват в секция Изпратени със статус Върнат и чрез маркирането им могат да се копират в секция За изпълнение, оттам да се редактират, запазят, потвърдят и/или повторно изпратят.

Банката препоръчва Потребителите ежедневно да проверяват статуса на нарежданията си.

Обработка в Банката

Банката обработва получените нареждания през Интернет Банкирането от 8.00 до 15.00 часа от понеделник до петък (без официално обявените почивни дни за Република България) по реда на тяхното постъпване в Банката.

Нареждания за превод, изпратени до 15.00 часа се обработват в същия работен ден. Постъпилите нареждания след този час се обработват на следващия работен ден.

Системата проверява за разполагаемостта по сметките, от които следва да се изпълнят нарежданията, по реда на тяхното постъпване. Те се изпълняват последователно, докато общата сума на изпълнените нареждания не надвиши наличността по съответната сметка.

- **Модул Депозити**

През модул Депозити потребителят може да извършва всякакви операции с депозити:

- Откриване на депозит;
- Увеличаване на депозит;
- Намаление на депозит;
- Закриване на депозит;

Минималната сума на депозита е 2,000 BGN/EUR/USD.

През модул Депозити Потребителят може да се запознае с Общите условия на Банката по договори за депозити, както и с валидния към момента Лихвен Бюлетин на Банката.

Инициирането, редакцията, потвърждаването, изтриването, изпращането на документ за депозит, както и неговият статус на обработка, са аналогични на описаните в точка 2 по-горе. Единствената особеност е, че при записване и потвърждаване на документ за депозит, същият отива в модул Депозити, секция За изпълнение, а изпратените към Банката депозитни документи се запазват в модул Депозити, секция Изпратени.

- *Откриване на депозит*

През Интернет банкирането на Банката могат да се откриват всякакви видове депозити: стандартни депозити, промоционални депозити и преференциални депозити (предварително договорени с Банката).

За депозити над 30,000 BGN/EUR/USD могат да се договарят преференциални условия (лихвен процент, срок „по мярка” на клиента, периодично олихвяване в рамките на срока на депозита и др подобни).

Откриването на стандартен депозит се извършва през документ Откриване на срочен депозит.

Откриването на промоционален депозит се извършва през документ Откриване на промоционален срочен депозит.

Откриването на преференциален депозит се извършва през документ Откриване на преференциален срочен депозит (депозит с параметри, предварително договорени с Банката), в който се разгръщат следните допълнителни полета:

- Тип срочност – указва се дали депозитът е месечен или дневен;
- Брой – указва се броят на месеците или дните, в зависимост от избраната стойност в горното поле;
- Лихвен процент – записва се договореният с Банката лихвен процент;

Във всеки документ за откриване на депозит, Потребителят следва да укаже параметрите на депозита: валута и сума; срок; сметка, от която следва да се захрани депозита; да потвърди, че е запознат и приема Общите условия на Банката по договори за депозити.

Откриването на стандартен и промоционален депозит (ако не се превалутира сума по предварително договорен курс) се извършва автоматично от Банката при получаване на документа за откриване. Откриването на преференциален депозит се извършва след обработка от страна на Банката и в тази връзка препоръчваме в края на деня Потребителят да провери статуса на изпратените депозитни документи.

Всеки новооткрит през Интернет банкирането депозит автоматично се регистрира за достъп през Интернет банкирането на Банката и Клиентът може да види параметрите му в модул Справки. Банката разпечатва и подписва договор за новооткрития депозит в два екземпляра, като запазва единия за себе си, а другия класира в Клиентската кореспонденция на Клиента.

- *Увеличаване на депозит*

Увеличаване на депозит, който не е на падеж се счита за нарушаване на условията по депозита и в този случай по депозита се прилага лихвения процент при предсрочно прекратяване на депозита, както и се оформя нов депозит със зададените от Потребителя параметри.

Увеличаване на депозит се извършва през документ Увеличаване на срочен депозит, където Потребителят следва да укаже: депозитната сметка, по която иска да довнесе сума; сумата, с която иска да увеличи депозита; срока на новия депозит; сметката, от която следва да се увеличи депозита; да потвърди, че е запознат и приема Общите условия на Банката по договори за депозити. Ако Клиентът е договорил с Банката новият депозит да е преференциален, в полето за Срок на новия депозит се избира Друг, при което автоматично се разгръщат следните допълнителни полета: Тип срочност (указва се дали депозитът е месечен или дневен), Брой (указва се броят на месеците или дните, в зависимост от избраната стойност в горното поле) и Лихвен процент (записва се договореният с Банката лихвен процент). Ако има договорени и други преференциални параметри, същите се описват в полето Пояснения.

Промоционалните депозити не могат да се увеличават от документ Увеличаване на срочен депозит. Ако все пак Клиентът желае да увеличи сумата по вече съществуващ промоционален депозит, той би могъл да го закрие от документ Закриване на срочен депозит и после да открие нов депозит за по-голяма сума от документ Откриване на срочен депозит.

В случай, че Потребителят е задал новооткритият депозит като стандартен депозит и сумата на увеличението не представлява обмяна на валута по предварително договорен с Банката курс, увеличаването се извършва автоматично от Банката при получаване на документа за увеличаване.

В случай, че Потребителят е задал новооткритият депозит като преференциален, увеличаването се извършва след обработка от страна на Банката и в тази връзка препоръчваме в края на деня Потребителят да провери статуса на изпратените депозитни документи.

Всеки новооткрит депозит автоматично се регистрира за достъп през Интернет банкирането на Банката и Клиентът може да види новите параметри му в модул Справки. Банката разпечатва и подписва договор за новооткрития депозит в два екземпляра, като запазва единия за себе си, а другия класира в Клиентската кореспонденция на Клиента.

- *Намаление на срочен депозит*

Намаляване на депозит, който не е на падеж се счита за нарушаване на условията по депозита и в този случай по депозита се прилага лихвения процент при предсрочно прекратяване на депозита, както и се оформя нов депозит със зададените от Потребителя параметри.

Новият депозит не може да пада под изискуемия минимум за депозити (2,000 BGN/EUR/USD).

Намаляване на депозит се извършва през документ Намаление на срочен депозит, където Потребителят следва да укаже: депозитната сметка, от която иска да намали сумата на депозита; сумата на намалението; срока на новия депозит; сметката, по която следва да се преведе сумата на намалението по депозита; да потвърди, че е запознат и приема Общите условия на Банката по договори за депозити. Ако Клиентът е договорил с Банката новият депозит да е преференциален, в полето за Срок на новия депозит се избира Друг, при което автоматично се разгръщат следните допълнителни полета: Тип срочност (указва се дали депозитът е месечен или дневен), Брой (указва се броят на месеците или дните, в зависимост от избраната стойност в горното поле) и Лихвен процент (записва се договореният с Банката лихвен процент). Ако има договорени и други преференциални параметри, същите се описват в полето Пояснения.

Промоционалните депозити не могат да се намаляват от документ Намаление на срочен депозит. Ако все пак Клиентът желае да намали сумата по вече съществуващ промоционален депозит, той би могъл да го закрие от документ Закриване на срочен депозит и после да открие нов депозит за по-малка сума от документ Откриване на срочен депозит.

В случай, че Потребителят е задал новооткритият депозит като стандартен депозит и сумата на намалението не представлява обмяна на валута по предварително договорен с Банката курс, намаляването се извършва автоматично от Банката при получаване на документа за намаляване.

В случай, че Потребителят е задал новооткритият депозит като преференциален, намаляването се извършва след обработка от страна на Банката и в тази връзка препоръчваме в края на деня Потребителят да провери статуса на изпратените депозитни документи.

Всеки новооткрит депозит автоматично се регистрира за достъп през Интернет банкирането на Банката и Клиентът може да види новите параметри по депозита в модул Справки. Банката разпечатва и подписва договор за новооткрития депозит в два екземпляра, като запазва единия за себе си, а другия класира в Клиентската кореспонденция на Клиента.

- *Закриване на срочен депозит*

Закриване на депозит, който не е на падеж се счита за нарушаване на условията по депозита и в този случай по депозита се прилага лихвения процент при предсрочно прекратяване на депозита

Закриване на депозит се извършва през документ Закриване на срочен депозит, където Потребителят следва да укаже: депозитната сметка, която иска да закрие и сметката, по която следва да се преведе сумата на закрития депозит.

Закриването на депозит се извършва автоматично от Банката при получаване на документа за закриване, освен ако операцията не представлява обмяна по предварително договорен с Банката курс. Банката разпечатва и подписва документ за закриването на депозита в два екземпляра, като запазва единия за себе си, а другия класира в Клиентската кореспонденция на Клиента.

- **Модул Настройки**

При избор на модел Настройки в лявото вертикално меню се визуализират следните опции:

- Регистрационни данни
- Промяна на парола
- Списък с TAH кодове
- Статистика

- *Секция Регистрационни данни*

При влизане в тази секция, на екран се визуализират: 1/ регистрираните Потребители за достъп до сметките на Клиента с информация за тяхното име, ЕГН, адрес, профил, лимит, потребителско име и статус и 2/ регистрираните сметки за достъп през Интернет банкирането. От тази секция Клиентът (само Потребител с профил А) може:

- да добави нов Потребител на Интернет банкирането със съответни права на достъп (профил и лимит) – чрез натискане на бутон Добави потребител и попълване на информация за съответния Потребител. При регистрацията на нов Потребител се попълва името и ЕГН-то на лицето, профила на Потребителя (A, B, C, D, E), лимитите, за които Потребителят е оторизиран, потребителско име и парола. Регистрираните Потребители с право да се разпореждат със сметките на клиента (профили А, В и С), трябва да имат нотариално заверено пълномощно, представено в Банката или пълномощно, попълнено пред служител на Банката.;
- да види статуса на всеки регистриран Потребител – чрез натискане на Покажи срещу съответния Потребител;
- да редактира съществуващ Потребител – влиза се в описанието на съответния Потребител, редактират се неговите параметри и се натиска бутон Добави;
- да блокира съществуващ Потребител - влиза се в описанието на съответния Потребител и се натиска бутон Блокирай;
- да разблокира Потребител – влиза се в описанието на съответния блокиран Потребител и се натиска бутон Добави;
- да добавя нови сметки за Интернет достъп - чрез натискане на бутон Добави сметка и попълване на номера на съответната сметка;
- да изтрива вече регистрирани сметки за Интернет достъп – чрез натискане на Покажи срещу съответната сметка;

При наличието на един от горецитираните случаи, Клиентът или упълномощено от него лице разпечатва и подписва Заявка за направените промени в регистрационните данни и я депозира в Банката за обработка и активиране.
Промяната на регистрационните данни, влиза в сила след обработката и активирането й от страна на Банката.

- *Секция Промяна на парола*

Тази точка позволява Потребителят да си сменя паролата. В секцията се съдържа информация и за броят дни, изтекли без промяна на използваната в момента парола.

С цел осигуряване на максимална защита на системата препоръчваме при първи вход и на всеки 60 календарни дни Потребителят да смени паролата си. Смяната на паролата е задължителна при първи вход в системата на Потребител, регистриран на гишетата на Банката. След изтичане на 60-дневния срок, системата предлага промяна на паролата. Съхраняването и опазването в тайна на потребителското име и парола от момента на активиране на услугата е лична отговорност на всеки Потребител.

- *Секция Списък с TAH-кодове*

От това меню се активират неактивните списъци с TAH-ове /всеки нов неактивен списък/, чрез въвеждане на последния 50-ти TAH от текущия активен списък и натискане на бутон Активирай. Изисква се и TAH №49 да е бил използван за подписване и изпращане на нареждания към Банката.

- *Секция Статистика*

В тази секция може да се проследи статистика на събитията, свързани със сигурността в системата за Интернет банкиране - по дата, час и електронен адрес на компютъра на Потребителя.

- **Модул Поща**

В модул Поща Потребителят може да види съобщенията, изпратени от Банката, както и да инициира съобщение до Банката в свободен формат (само Потребители с профили А), което изисква въвеждане на ТАН.

- *Съобщения от Банката*

Банката периодично изпраща на клиентите съобщения, с цел Клиентът да бъде своевременно информиран за, нови услуги, промоции, новини и други събития, свързани с Банката. Списъкът с входящите съобщения е организиран по дата, подател на съобщението и тема.

- *Съобщения до Банката*

Потребител с профил А може да изпрати съобщение до Банката в свободен текст от секция Съобщения до Банката, За изпращане и натискате бутон Изпрати съобщение до банката. След написване на съобщението, Потребителят има възможност да го запише за последващ преглед/редакция или директно да го изпрати към Банката чрез въвеждане на ТАН. Информация за изпратените към Банката съобщения може да се намери в секция Съобщения до Банката, Изпратени.

- **Модул Информация**

Системата Интернет банкиране предоставя следните информационни услуги на клиентите:

- *Информация за актуалните валутни курсове на Банката и фиксинга на БНБ;*

При избор на тази точка се визуализира информация за:

- фиксинга на БНБ по дати за евро, щатски долар и паунд;
- валутните курсове на Банката за текущия ден (купува и продава);
- валутен калкулатор;
- възможност за справки за фиксинга на БНБ за зададен от потребителя период;

- *Лихвен бюлетин на Банката;*

При избор на тази точка се показва актуалния Лихвен Бюлетин на Банката.

- *Банки-кореспонденти;*

При избор на тази точка се визуализират банките-кореспонденти, чрез които се извършват валутни преводи по нареждане на и в полза на клиентите на Банката с информация за името и суифта на банката-кореспондент, валутата и сметката на БАКБ.

- *Общи условия;*

При избор на тази точка се визуализират актуалните Общи условия на Банката:

- Общи условия за ползване на услугата Интернет банкиране на БАКБ;
- Общи условия за предоставяне на платежни услуги;
- Общи условия за деловата дейност на БАКБ;
- Общи условия по договори за депозит;

- *Други*

Обновяването на информацията в Интернет банкирането става до 5 минути в рамките на работния ден на Банката без събота.

Ако в сесията за интернет банкиране не се работи 20 минути, сесията се затваря автоматично.

След приключване на работа със системата за Интернет банкиране, задължително следва да се използува бутон "Изход", за да се затвори активната връзка с Банката. По този начин се елиминира възможността за неоторизиран достъп или злоупотреба от работната станция на потребителя.

3.13.Технически изисквания

За да се използва услугата Интернет банкиране е достатъчно клиентът да има достъп до интернет от произволна работна станция. Не са нужни допълнителни технически и софтуерни средства.

Препоръчително е избраната от клиента работна станция да е със следните или по-високи параметри:

- Интернет браузър MS Internet Explorer 7 или Mozilla Firefox 2.0 или по-високи версии. Актуална версия на предпочитания от Вас браузър може да намерите на сайта на производителя - http://www.microsoft.com/downloads/en/default.aspx или http://www.mozilla.com/en-US/products/download.html
- Операционна система – всички поддържащи на някой от горецитираните браузъри
- Връзка с Интернет.

3.14. Мерки за сигурност при интернет банкирането

- ***Уеб сигурност; Защита на информацията;***

По подразбиране, комуникациите през Интернет са отворени и неконтролирани. Този факт е в конфликт с нуждите на цифровия бизнес, който изисква конфиденциалност и цялост на транзакциите. Все по-широкото приложение на електронния бизнес поставя на преден план въпроса за сигурността. Сигурността в Интернет прераства във въпрос, касаещ бизнес стратегията на всяка компания. Тази сигурност не е само технически проблем, който трябва да се реши на ниво IT отдел в дадена компания.

Понастоящем технологията може да обезпечи системната сигурност, но за целта е необходимо да се използва нещо повече от обикновена технология. В случай, че разгледате по-детайлно причините за тези проблеми ще видите, че в повечето случаи те се крият в човешки грешки, липсващи процедури и неправилно конфигуриран софтуер. Тези грешки не могат да се елиминират дори и с най-добрата технология, а само с цялостна корпоративна стратегия за сигурност.

Основният проблем в Интернет е идентифицирането на потребителите. В един магазин купувача се идентифицира със своя външен вид, но в Интернет това не е възможно. Въпреки, че в реалния живот даден човек може да се представи за друг, в Интернет това е още по-лесно. В Интернет никой не може да бъде сигурен за идентичността на друг човек, освен ако не се използва допълнителна технология. Но дори и даден човек да може да бъде идентифициран, често той не може да участва в бизнеса, тъй като му е необходим подпис който не може да се направи без участието на юридическа организация. Сигурността на информацията е най-важното нещо в Интернет, но тя не може да се осигури, ако има пропуски във фундаменталните принципи.

За да се обезпечи сигурността на информацията е необходимо да се избегне неоторизирания достъп до електронните данни, в критичните от гледна точка на бизнеса системи в дадена компания. Резултатът от неоторизиран достъп може да бъде промяна, заместване, разпространение или нарушаване на дадена информация.

Организациите и хората, които използват компютри могат да опишат своите нужди за сигурност на информацията от гледна точка на пет основни изисквания: конфиденциалност, цялост, наличност, легитимност и липса на отказ. Конфиденциалността е необходима за да се контролира получателя на дадена информация и за да се избегне нейното разпространение. Целостта трябва да гарантира, че информацията и програмите се променят само по определен и оторизиран начин, че данните са действителни и не са променени или изтрити по време на предаване. Наличността трябва да гарантира, че оторизираните потребители имат непрекъснат

достъп до информацията и ресурсите. Легитимното използване означава, че ресурсите не могат да се използват от неоторизирани потребители или по неоторизиран начин.

Тези пет компонента могат да бъдат оценявани по различен начин в зависимост от конкретното приложение. Необходимо е да се прави оценка на риска за да се определи каква тежест да се придаде на всеки от тях. За обезпечаване на сигурност на информацията могат да се използват различни технологии.

Конфиденциалността и целостта могат да се изпълнят чрез криптографски методи, които осигуряват висока степен на сигурност. Чрез криптиране на данните никой не може да каже какво точно съдържа дадена информация. Посредством строго идентифициране може да се гарантира, че никой не вижда, не копира и не изтрива дадена информация. С комбинация от идентифициране и криптиране, единствения начин за достъп до данните е да се притежава необходимия сертификат за идентифициране и ключа за криптиране. Една система за идентифициране може да откаже достъп на оторизирани хора, които се опитват да получат достъп до информацията по неоторизиран начин. Липсата на отказ изисква намесата на трето лице, което отбелязва момента на входящата и изходяща комуникация, и което може да проверява валидността на цифровия сертификат. Когато е известен момента от време, в който дадена информация е влязла или излязла може да се провери дали дадена електронна поща е изпратена навреме.

Това, на което трябва да се обърне внимание при осигуряване на защитата са ключа за криптиране, възлагането на отговорност, отговорността за даден ключ и одит на достъпа. Няма съмнение, че една правилно изпълнена криптографска система, която се управлява коректно предлага най-високата степен на сигурност на електронната информация.

За разлика от онлайн магазините, при електронното банкиране една парола не осигурява достатъчно спокойствие нито за клиента, нито за банката. За да активирате изобщо услугата, трябва първо лично да отидете до офиса на банката, да покажете лична карта, и да положите собственоръчно подпис.

В DBank например отпечатват списък с еднократни кодове за сигурност. При първото влизане използвате първия код, при второто обаче той вече е невалиден и трябва да въведете втория и т.н..

Някои банки имат изискване паролата, която ще си ползва, да съдържа задължително букви и цифри (при това сред буквите трябва да има и главни). Това определено повишава сигурността на паролата и намалява шанса тя да бъде разкрита.

При влизане в интернет страницата им някои банки ви подсещат да си смените паролата или направо ви изтриват досегашната и искат да си измислите нова. Или ако искате пак си въвеждата старата – един вид като потвърждение, че още се използва.

ЦКБ например не дава интернет банкиране, ако клиента няма електронен подпис. ДСК пък задължително издава електронен сертификат за сигурност.

Също така сайтовете за онлайн банкиране обикновено ползват подсигурения протокол HTTPS (това е стандартния HTTP (Hyper Text Transfer Protocol) + SSL (Secure Sockets Layer)). Той криптира целия трафик – цялата информация, плюс паролата за достъп – правейки почти невъзможно за трети лица да се сдобият с тях. Все пак протоколът криптира само трафика и ако клиентският компютър не е добре защитен, паролата може да бъде „подадена" на трети лица директно по време на въвеждането. Това се осъществява чрез програми, които се наричат кий логъри (на английски: key loggers), които записват натиснатите клавиши. Съществуват и физически устройства със същите функции, които често се използват не по предназначение. Разбира се, остава и опасността от „разбиване" (или отгатване) на недобре подбрани пароли, както и кражбата им, ако са били записани някъде.

За България като допълнителна сигурност се практикува използването на достъпа до онлайн услугите само чрез един фиксиран компютър, както и транзакционен авторизационен номер - TAH, който представлява шестцифрен код, който се използва от потребителите еднократно за подписване на нарежданията към банката. Обикновенно се получава чрез СМС по телефона.

Би трябвало страницата за е-банкиране да започва не с “http” както повечето интернет страници, а с “https“.

Проблемите на сигурността при интернет банкирането са свързани най-вече с това да се заблудят клиентите, наример с фалшиви мейли представящи се като изпратени от самата банка или уеб сайт имитиращ реалния банков сайт с цел кражба на данни и клиентски потребителска имена и пароли.

- ***Електронен подпис***

Друг начин за подобряване на сигурността е използването на електронен подпис или токен устройство.

Електронния подпис (англ. Digital Signature) е реквизит на електронен документ, предназначен за защитата му от фаршификация. Това е криптографски подпис или по-точно математическа функция, получена в резултат на криптографска обработка на информацията, извършена с цел да се удостовери самоличността на изпращача и да се гарантира, че информацията не е била променяна по пътя между изпращането и получаването. Електронните подписи се използват при дистрибуция на софтуер, при финансови транзакции и навсякъде където се обменя важна информация по електронен път и е важно евентуално фалшифициране или опит за фалшифициране да бъдат открити навреме.
Електронния подпис използва за криптирането алгоритъм, с една степен по-сигурен от алгоритмите, използващи хеш-функция за удостоверяване на самоличността на изпращача. Използва се асиметрична криптография с двойка ключове – частен и публичен, като единия се криптира, а с другия се декриптира. [9]

Българския Закон за електронния документ и електронния подпис (ЗЕДЕП) дава следното определение:

„Електронно изявление е словесно изявление, представено в цифрова форма чрез общоприет стандарт за преобразуване, разчитане и визуално представяне на информацията. Електронното изявление може да съдържа и несловесна информация.

Електронен документ е електронно изявление, записано върху магнитен, оптичен или друг носител, който дава възможност да бъде възпроизвеждан. Електронен подпис е всяка информация в електронна форма, добавена или логически свързана с електронното изявление, за установяване на неговото авторство.“

Съществуват два вида електронни подписи: Усъвършенстван и Квалифициран.

Усъвършенстван е този електронен подпис който:

- ✓ Дава възможност за идентифициране на автора;
- ✓ Свързан е по уникален начин с автора;
- ✓ Създаден е със средства, каито са под контрола единствено на автора;
- ✓ Свързан е с електронното изявление по начин, който осигурява установяването на всякакви последващи промени;

Квалифициран е усъвършенстван електронен подпис, който отговаря на две допълнителни условия:

- ✓ Придружен е от издадено от доставчик на удостоверителни услуги удостоверение за квалифициран електронен подпис, удостоверяващо връзката между автора и публичния ключ за проверка на подписа;
- ✓ Създаден е посредством устройство за сигурно създаване на подписа;

Квалифицираният електронен подпис има значението на саморъчен подпис.

- ***Токен устройство – предимства и функционалност***

Токен устройство (също така се ползват термините като хардуерен токен, удостоверяващ токен, USB токен, криптографски токен, софтуерен токен, виртуален токен или ключ), представлява физическо устройство, което позволява на оторизиран юзър на компютърна система да се идентифицира. Тези условия се отнасят също така и за софтуерни токени. Токенът е хардуерно устройство, което всеки път генерира нова парола. Изписана след ПИН кода, тя предоставя достъп до банковата сметка.

Токенът може да служи само за нареждане на банкови операции, но също така и да се използва като вход за изначален достъп до виртуалното банкиране. Така електронното банкиране ще бъде неизменно обвързано с устройството винаги.

Паролата

Паролата от Token се състои от два компонента. Първият се нарича ПИН. Той се получава още, със закупуването на устройството от банковия клон. ПИН-ът е шестцифрен код, който обслужващата банка изпраща по имейл и който е хубаво да се промени, за да не станат злоупотреби при хакване на личния имейл или друга лична информация.

Вторият компонент е *ключовата роля на Token-а*. Това е втора шестцифрена парола, която се генерира с всяко натискане на бутона на Token-а и всеки път е различна. Така, заедно с ПИНт-а, паролата става 12-цифрена, като всеки път последните 6 цифри са различни. Освен това без Token устройството тези цифри не могат да се появят на екрана. Именно затова Token-ът носи сигурност за потребителите. Той е като двойно заключващо устройство с променлив механизъм за вашите електронни пари. И може да бъде отключено само от ползващия го потребител.

Токенът ще блокира след 5 въвеждания на грешни пароли, но чрез въвеждане на специфични данни можете да бъде деблокиран. Най-важното обаче е да не се забравя ПИН-а, защото в повечето случаи това налага смяна с ново устройство

Има и банки, в които не се налага закупуването на нов Token след посещение на банков клон. В клоновете на Fibank например могат да издадат нов ПИН код.

Устройството има и гаранция. Така например във Fibank този срок е две години. В този срок, ако устройството не генерира пароли, ще бъде подменено безплатно на клиента, стига да не са на лице следи от механичен проблем – притискане, счупване, намокряне и други от такова естество.

Самият Token може да генерира до 10 000 сесийни пароли, което означава, че животът на устройството зависи от честотата на ползването му. Но колкото и изтензивно да е то, съвсем лесно можете да бъде закупен нов Token.

Сред предимствата на Token-а е, че не е необходимо да се инсталира нищо, за да работи, за разлика от Квалифицирания Електронен Подпис (КЕП).

Ако все пак клиента вече притежава КЕП, но желае по-лесно и удобно банкиране през мобилния си телефон, то може да се обърне към обслужващата си банка, за да настроят Token-а за достъп само до мобилния ви телефон или за средство за допълнителна сигурност. По този начин освен КЕП ще може да се използва и Token, за да влизане в системата за банкиране.

Предимства на Токен устройствата

Еднократните (сесийни) пароли дават по-голяма сигурност, защото са валидни само за една-единствена сесия или определен период от време

Евентуално хакване на паролата няма да даде достъп до сметките на клиента. Token-ът е малко компактно устройство с размера на обикновена флашка, лесно и удобно е за употреба.

Лесно за пренасяне. Дава сигурност за безрисково банкиране. Не представлява сериозен разход. Може да работи с различни браузери. Също така работи с таблети и мобилни телефони.

3.15.Информационна политика

За да гарантира сигурността на най-важната информация, всяка компания трябва да разработи информационна политика, която да гарантира правилното изпълнение на процесите, когато нещо се случи. Процесът на разработване на информационна политика е като кръг, който винаги ви връща до началната точка. Разбира се, не можете да очаквате, че всичко ще работи от първия път. Новите технологии и идеи изискват непрекъснато да обновявате информационната политика. Така както вашата web страница изисква непрекъснато обновяване, така и процесите за обезпечаване на сигурността изискват непрекъснато обновяване.

Първата стъпка във вашата информационна политика е да направите списък с всички ресурси, които трябва да бъдат защитени. В този списък трябва да включите компютри, принтери, маршрутизатори, защитни стени, сгради, където се намира хардуера или където се съхраняват вашите архивни копия. Трябва да се определи кой получава физически достъп до хардуера и логически достъп до софтуера често физическия достъп се пропуска да бъде отбелязан, но дори и най-добре защитения софтуер става безпомощен когато хакер влезе в сградата и изкопира върху дискета или CD-ROM диск необходимите му файлове.

След като се направи списък на всички ресурси, трябва да се опишат вероятните заплахи за всеки ресурс. След като се направи и този списък, трябва да се направи оценка на риска, която показва в проценти вероятността от реализиране на всяка заплаха. Поради факта, че не е възможно да се инвестира във вземане на мерки срещу всяка заплаха, компанията трябва да прецени кои заплахи могат да се пренебрегнат за момента и на кои трябва да се обърне сериозно внимание.

За да избегнете най-вероятните причини за нарушаване на сигурността трябва да реализирате рентабилна система за сигурност. При системите за сигурност, много важен фактор са разходите свързани с реализацията им. Сигурността не може да се оценява по възвръщаемост на инвестициите. Изпълнявайки една система за сигурност вие правите разходи, които никога не могат да бъдат възстановени. Единственото нещо, което може да се каже е, че е твърде вероятно при отсъствието на тази система компанията ви да загуби доста средства и клиенти, но в същото време е много трудно да убедите мениджърите от високо ниво, че се налага да инвестират много средства за обезпечаване сигурността на информацията.

За да не пропуснете появата на нови заплахи, трябва непрекъснато да проследявате нещата и да обновявате своята система за сигурност. По този начин ще гарантирате наличието на стабилна система за сигурност, която ще ви предпазва от неоторизиран достъп.

3.16.Заплахи в Интернет

Повечето заплахи в Интернет могат да се класифицират в една от следните четири категории:

- ***Загуба целостта на данните*** - Нарушителят добавя, модифицира или изтрива информация;
- ***Загуба на конфиденциалност на данните*** - Информацията става достъпна за неоторизирани потребители;
- ***Загуба на услуги*** - в резултат от действията на хакера, дадена услуга вече не може да се изпълнява;
- ***Загуба на контрол*** - Услугите се използват от оторизирани потребители по неоторизиран начин;

Много хора се опитват да намерят слаби места в софтуера или конфигурацията, за да могат да влезнат в системата. Често онлайн банките са целта на хакерите, тъй като идеята за трансфер на пари е значителна мотивация за много хора. В някои случаи хакерите не искат да получат достъп до системата, а просто да предизвикат така наречения „отказ за изпълнение на услуга" („Denial of Service - DoS"). Целта на DoS е да се откаже достъпа на оторизирани потребители до системата. Това може да стане посредством атакуване на мрежови компоненти, като маршрутизатори или компютърни системи, чрез атакуване на определени

приложения или операционната система. Това води до прекъсване работата на системата, което може да доведе до финансови загуби на потърпевшата компания.

Съвременните технологии за обезпечаване на сигурността затрудняват действията на хакерите, но всеки ден се публикуват нови уязвими места в приложния софтуер и операционните системи, с което се предлагат нови възможности за хакерите. За да може една система да има гарантирана сигурност е необходимо операционната система и приложния софтуер да се обновяват регулярно.

Има много начини, по които може да се атакува една система. Един от тези начини е например, да се наблюдава комуникацията между двама партньори. По подразбиране, комуникацията през Интернет е абсолютно незащитена и информацията се предава като прозрачен текст. Чрез наблюдение на комуникацията може да се извлече конфиденциална информация и пароли. Ако например, осъществите достъп до вашия mail сървър, името на потребителя и паролата се изпращат до сървъра и всеки в Интернет може да ги прихване. Ако даден хакер успее да прихване това, той може да промени информацията преди тя да е стигнала до предназначеното местоположение. В случай, че получателя няма специален софтуер, той няма да забележи промените направени от трето лице.

Една друга възможност за неприятности е софтуера или хардуера да бъдат откраднати. Софтуер, като например бази данни може да съдържа конфиденциални данни и пароли, а хардуера може да даде възможност на хакера да разбере как е изградена вътрешната мрежа. Освен това, при достъп на хакери до хардуера те могат да разберат фабрично кодираната в отделните хардуерни модули информация, като например код на смарт карта, посредством който може да се разбере по какъв начин се използва тази карта.

Освен прихващане на мрежови комуникации, могат да се прихващат и електромагнитни изходни сигнали от устройства, като например монитори. Съществуват устройства, които могат да копират съдържание, показано на екрана на един монитор върху друг монитор, който се намира на разстояние стотици метри. Реализирането на „отказ за изпълнение на услуга" може да стане чрез атакуване на уязвими места в операционната система или приложен софтуер, или когато дадена услуга просто се претовари с прекалено много заявки. В последния случай, системата е заета с обслужване на тези заявки и отказва изпълнението на легитимните заявки.

"Троянските коне" са друг метод за нелегитимно проникване в дадена система. Обикновено „троянският кон" е скрит в безобидно изглеждащ софтуер, който го активира при стартирането си. „Троянският кон" работи на заден план и събира информация за системата и нейните потребители. След това, тази информация се изпраща на хакера, който може да влезе в системата и да я контролира отдалечено. Друг известен тип атака е „маскирането" (известно още като „лъжливо представяне"). Представяйки се за друг потребител, хакерът може да влезе в системата. Повечето атаки се изпълняват с лъжлив IP адрес. Много системи позволяват достъп до ресурсите само на ограничен набор IP адреси. Хакерът показва IP адрес точно от този набор, при което получава автоматичен достъп до определени ресурси. Много системи игнорират заявките от системи с неоторизирани IP адреси. С помощта на лъжлив IP адрес, дадена система може да се покаже като оторизирана за осъществяване на достъпа. Въпреки че при представянето на лъжлив IP адрес няма да се дадат автоматично права за достъп, хакера има възможност да види необходимата му информация. При представянето на лъжлив IP адрес, системата до която се изисква достъп ще започне да отговаря на заявките на хакера и по този начин ще му даде възможност да атакува повече неща.

Друг начин за получаване на информация от дадена система е да се погледне в кофите за боклук, които се намират пред сградата на офиса на дадена компания. Често служители изхвърлят дискети, които могат да съдържат информация, която да помогне на хакерите при влизането в системата. При атаки осъществени по този начин е по-лесно да се открият хакерите, тъй като се предполага, че те се намират близко до офиса на компанията.

Друг начин за получаване на достъп до паролите и вътрешната архитектура на системата, обезпечаваща сигурността на информацията е като се подкупи някой служител. Често когато на някои служители им се предложат пари, те са готови да дадат информация за начина на достъп до системата и до конфиденциална информация. Въпреки че не е възможно да контролирате всеки един от своите служители, системата за сигурност никога не трябва да

зависи от един единствен служител. Много е важно повече хора да са запознати с нея, за да може да се реагира в случаите когато даден служител е болен или пък напусне компанията.

Физическият достъп е по-традиционен начин за получаване на информация или нарушаване работата на дадена услуга. В този случай, атакуващият влиза в сградата, преминава безпрепятствено през системата за контрол на достъпа и просто си взима необходимата информация. Това изисква атакуващия да бъде физически близко до мястото от където ще взема информацията. Това често помага да се разкрие хакера и понастоящем този тип атаки са почти невероятни.

Във връзка с лъжливите IP адреси много хакери не само че дават лъжлива информация, но и събират информация, като например пароли. Представете си, че любимия ви онлайн магазин за книги в Интернет получи лъжлив IP адрес. Когато влезете в URL на този магазин, името на домейна се свърза с неверния IP адрес и ви показва неправилна home page. Повечето професионални хакери копират съдържанието на web страницата на ново място и препращайки потребителите към новия сайт събират информация за тях. Когато даден потребител си избере определени книги, които ще закупи, посредством неговите име и парола може да се осъществи достъп до съществуващите му банкови сметки. В случай, че тази информация попадне в ръцете на хакер може да си представите какво той може да направи, докато потърпевшия разбере и предприеме мерки.

Друг начин, по който хакерите могат да се допуснат до системата е като им се предостави информация за вътрешната мрежа. Много компании използват имена на домейни от типа „system01.domain.org", „ "system02.domain.org ", „ system03.domain.org " и т.н. Това може да помага на персонала да брои наличните системи, но улеснява хакерите, които разбират кои компютри са включени и какви са техните имена. Повечето компании използват като домейн за външен web сървър име от типа www.domain.org, но www често е псевдоним за име на реална система. Срещал съм системи, които се наричат „xxx07domain.org" и в същото време са външен web сървър. Написвайки „telnet xxx01.domain.org" лесно може да се разбере дали други системи са директно свързани към Интернет и с каква операционна система работят. Друга слабост на някои компании е, че дават възможност на външния свят да вижда вътрешната им DNS структура. В случай, че никой не може да вижда вътрешната мрежа, тогава никой няма да знае за какво се използва всяка една от системите в тази структура.

3.17.Социално инженерство

Повечето сложни и успешни атаки не са свързани с техническо проникване в дадена система, а имат социален характер. Вместо да се използва технология за влизане в дадена система, социалното инженерство опитва да намери хора, които да изпълнят заявките на атакуващите. Това не означава, че вие можете отдалечено да контролирате техните мисли и намерения. Социалното инженерство използва навиците на хората по такъв начин, че те да не разберат, че някой е получил от тях някаква информация.

Повечето атаки се осъществяват, като хакера се представя за някой друг. Това разбира се включва повече от просто обаждане до IT отдела на дадена компания и поискване на паролите за компютрите, на които се намират защитния софтуер. Въпреки, че може да не повярвате на това, всичко може да завърши само с един телефонен разговор, ако е подготвено добре.

Социалното инженерство акцентува върху най-слабата връзка при Интернет сигурността - човека. За да бъде защитена една система, тя не трябва да бъде свързана към Интернет. Но дори и това не може да гарантира, че системата наистина ще бъде сигурна. През април 1999 г. хакери успяха да откраднат информация от институт за ядрени изследвания в САЩ, като използваха вътрешен човек, който изкопира необходимата им информация върху дискета.

Много бизнес компании разчитат на Интернет, а в бъдеще почти всички компании ще искат да участват в Интернет бизнеса. От тук се вижда, че всяка една от тези компании може да се окаже цел за хакерите. Социалното нахлуване улеснява хакерите, тъй като то не зависи от платформата, от операционната система или от приложния софтуер на системата на хакера.

Социалното хакерство работи по индиректен начин. Всеки, който има връзка с хора, познаващи системата за защита на информацията на дадена компания, може да се разглежда като потенциален риск за сигурността. С едно обаждане на секретар могат да се разберат имената на хората, работещи в дадена организация, от които може да се получи допълнителна информация. След няколко телефонни разговора, които не могат да се проследят, така както могат да се проследят електронни пощи, хакера получава достатъчно информация за компанията и нейните процедури на работа, така че просто може да се обади на някой от отдела по сигурност и да се представи за даден служител от компанията.

Събраната информация е като малки части от пъзел, които изглеждат съвсем незначителни за този, който предоставя информацията. Само че събрана като цяло, тази информация може да се използва за атаки срещу компанията. За да получи необходимата информация, необходимо е този, който я събира да се адаптира към вътрешните за компанията процеси. Схемите показващи структурата на компанията и телефонните указатели може да се окажат нещо доста полезно. Вътрешните документи, които се изхвърлят, винаги трябва да се късат, за да не може случаен минувач просто да си извади от кофата за боклук. Понастоящем използването на дискети трябва да се елиминира изцяло. Информацията от форматирана дискета може да се възстанови лесно. Твърдите дискове и дискетите, които вече не се използват в дадена компания трябва да се унищожават изцяло. Социалното инженерство не изисква задълбочени компютърни познания и дава възможност на всеки да се превърне в хакер.

Друг метод за получаване на информация е просто тя да се поиска директно. Просто можете да се обадите на администраторите и да поискате паролите за системата, обезпечаваща защитата на информацията. За да имате успех трябва да имате поглед върху структурата на компанията. Хакерът, например може да разбере, че някой мениджър на компанията, която смята да атакува е просто в друга държава, която е в часова зона различаваща се с осем часа от тази на държавата, в която е неговата компания. Да предположим, че този мениджър ще изнася реч в тази държава. Тогава хакерът може да се обади в офиса половин час преди речта на мениджъра и да попита за паролата, защото преносимия компютър, на който е презентацията не работи. Поради разликата в часовата зона, най-вероятно в държавата където е офиса на компанията да е нощ и само дежурните служители да бъдат на работа. Хакерът може да се представи за мениджъра и да поиска информацията да му бъде предоставена веднага, за да не закъснее със своята реч. За да убеди служителите, че той е този, за който се представя той може да поиска да говори с ръководителя на IT отдела.

Представете си този случай. Ако вие сте на мястото на този, от който се изисква да даде паролата ще го направите ли? През работно време може би ще направите някои проверки, но през нощта, когато сте сънен най-вероятно ще дадете исканата от вас информация без да се замислите. Социалното инженерство събира информация и оказва социален натиск. Една от често използваните стратегии е да се получи информация от служител, който очаква да бъде уволнен.

Хакерите използват силни аргументи когато правят последната стъпка от своята атака, тъй като слабите аргументи могат да породят съмнения. Когато се представят силни аргументи повечето хора се подчиняват. Този вариант ще има добър успех, особено ако човека, който се атакува е по-малко компетентен от хакера.

Както виждате, когато в администрирането на една система участва фактора човек, дори и тази система да има най-добрата защита, тя може да бъде атакувана индиректно. За да намалите верността вашата система да бъде атакувана посредством социално инженерство, трябва да обучите всички служители във вашата компания. Всеки един служител трябва да разбира важността на сигурността и да знае какви са методите използвани от хакерите. В много случаи е по-лесно да се получи информация от тези, които работят с компютрите, отколкото от самите компютри. В същото време е истина, че е по-лесно да се принудят служителите да не дават информация, отколкото да защитите даден компютър. Изводът от това е, че е необходимо непрекъснато обучение на служителите.

3.18.Защита разчитаща на неизвестност

Много компании ограничават разпространяването на информация, свързана със системите за сигурността. Избягвайки темите на разговор, свързвани със сигурността, голяма част от компаниите вярват, че нищо не може да им се случи. Други компании се опитват да скриват информация на своя web сървър, който може да се посещава от определена група потребители. Някои пък държат отворени за всеки, своите екстранет мрежи като разчитат на това, че ако дадат своя URL на определени потребители, никой освен тях няма да може да намери необходимата му информация. Други компании мислят, че тяхната технология обезпечаваща сигурността е толкова сложна, че никой няма да може да я разбере и да злоупотреби с нея.

Практиката доказа, че тези принципи са грешни и много експерти по сигурността смятат, че трябва да се провеждат отворени дискусии и обучение относно концепциите и технологиите за сигурност. Откритата дискусия за стандартите за сигурност е ключа към успешните технологии, така както отворените дискусии за Интернет технологията доведоха до успеха на Интернет.

Обезпечаване на сигурност посредством неяснота все още е доста прилагана стратегия при много компании, които се опитват да избегнат пропуските при обезпечаване на защитата. Разпространителите на софтуер се надяват, че като избягват въпросите за сигурността никой няма да документира пропуските и уязвимите места от гледна точка на сигурността в даден софтуер. Най-добрите продукти осигуряващи защита/сигурност се дискутират свободно и открито, и дори изходния код на продуктите може да се види от всеки Първоначално това може да ви се види странно, защото хакерите могат също да видят как работят алгоритмите. Само че по този начин и трети страни могат да видят кода и дори да го подобрят. Това изисква разпространителят на софтуера за защита да разработи алгоритми, които осигуряват силно криптиране без да може да се инвертира действието на алгоритъма. Един много добър пример е Pretty Good Privacy (PGP) където процесите и алгоритмите са документирани, без това да намалява степента на защита.

3.19.Решаване на въпросите със сигурността

Първият тип атака е отказ за изпълнение на услуга. Повечето от този тип атаки се правят като се атакува индиректно услугата - обект на атаката. В много случаи се атакува друга услуга, която е стартирана на същата система и за която се знае, че има слаби места. Например, един web сървър трябва да блокира всичкия трафик, който не е HTTP. Игнорирайки трафика на всички останали портове, освен порт 80 за HTTP, сървъра е по-малко уязвим към този тип атаки и не губи процесорна мощност за обработва на нелегитимни заявки за услуги от web клиенти.

За голяма част от цифровия бизнес друга също често срещана заплаха е „маскирането". Представяйки се за легитимен потребител, нахлуващия може да получи достъп до конфиденциална информация и изпълними команди, които не са достъпни за общата публика. В повечето случаи проблема тук е в това, че идентифицирането е базирано на един фактор, като парола или пин код. Последните две могат лесно да се изкопират. За да се направи идентифицирането сигурно то трябва да бъде двуфакторно. Това означава, че е включен не само фактора „нещо, което потребителя знае", но и фактора „нещо, което потребителя има". С използването на смарт карта с пин код, атакуващите трудно могат да се представят за някой друг, защото трябва да се преминат две независими бариери, преди да бъдат допуснати до системата.

Въпреки, че двуфакторното идентифициране е доста по-сигурно, все още има възможности за неоторизирано влизане в системата, физическият токен, като например смарт карта съдържа „тайна", която се използва за допускане на потребителя до системата. Тази „тайна" се отключва с помощта на пин кода. За да получат достъп до системата, атакуващите трябва да знаят „тайната" или да притежават тази смарт карта и пин кода.

За да не позволите на хакери да разберат „тайната" трябва да направите така, че физическия токен да не може да се фалшифицира. За да избегнете улавянето на пакета, „тайната" никога не трябва да напуска токена и не трябва да е възможно нейното прочитане. За да направите един физически токен уникален, е необходимо да се направи връзката между

приносителя на токена и неговия притежател. За да се избегне прихващането на пин кода, неговата валидност трябва да се отбележи върху самата карта. Това изисква клавиатурата от която се въвежда пин кода да е директно свързана с токена, за да се гарантира конфиденциалността на информацията.

Една регулярна проверка на log файловете на защитната мрежа, на web сървърите и на сървърите за приложения помага да се избегне фалшивото идентифициране. Един log файл трябва да записва всички неуспешни опити за влизане в системата и в случай, че броя на тези опити е голям, трябва да се стартира процес за контрол на идентифицирането.

Друг тип атака е прихващането на DNS, което позволява на хакерите да пренасочат клиентите към друг сървър и да получат важна информация за тях. За да се гарантира, че сървъра, с който се свързва даден клиент е правилния, трябва да се добави идентифициране на сървъра. Това се постига като на сървъра се постави цифров сертификат, който е уникален за всяка комбинация от име на домейн и IP адрес.

За да се избегне промяната на информацията по време на предаването и, трябва да се активира проверка за цялост на съобщението. Това се постига като към електронната поща се добави hash код (случаен/разбъркан код). Кодирането на съобщението помага за избягване на подслушването и за запазване на конфиденциалността му.

Един от големите проблеми в Интернет е отхвърлянето на съобщения, като в същото време се появява съобщение, че пощата е изпратена или приета. Това се прави често при бизнес транзакциите, като например онлайн поръчки и плащания. Хората често купуват стоки и след това отказват да платят. За да се гарантира отсъствието на отказ за плащане, трябва да е сигурно, че се приемат само поръчки, които ще се платят. Това се постига с използването на цифрови сертификати, които идентифицират клиента по сигурен начин.

3.20.Оторизиране

За да се прехвърли даден бизнес от частна мрежа към Интернет, трябва да се решат няколко въпроса, свързани със сигурността. Първо трябва да се определи кой и до какви бизнес приложения трябва да има достъп. Освен това е необходимо да се реши кой ще има достъп до конфиденциалната за дадена компания информация. При много видове бизнес няма ясна политика относно достъпа. Резултатът от това е, че е трудно да се определи от къде и кой е разпространил дадена информация. Списъкът с оторизираните потребители трябва да включва информация за това какви права има всеки потребител и да се определят точно приложенията, до които има достъп.

За да може този списък да се приведе в действие, компанията трябва да разработи и изпълни набор от политики за всички потребители на дадена система (т.е. служители, клиенти и партньори) и нейните приложения. Трябва да се изпълни общ процес на идентифициране.

По принцип, оторизирането се осъществява от система, която предпазва услугите и данните от неоторизиран достъп чрез строго наложени правила за това какво се позволява на даден потребител и какво не. Първата стъпка трябва да е преминаване от разпределено администриране на оторизирането към централизирано администриране. Повечето приложения имат свои собствени методи за прилагане на оторизирането. Поради факта, че все повече и повече приложения започват да се предлагат в Интернет, този разпределен модел е все по-неприложим за обезпечаване на сигурността, тъй като всяко приложение може да има различни бъгове, които да позволят достъп до него. Цените за разработка на нов софтуер са много високи, защото трябва да се включат нови модули за оторизиране. Централизираното администриране намалява разходите за реализация и поддръжка. Това позволява на администраторите да имат по-регулярен поглед върху политиките на сигурност.

Трябва да се поддържа списък на всеки ресурс (като например принтер, файл, база данни или приложение), както и на потребителите/групите, които имат достъп до него. С новата идея за използване на централизирана директория за администриране, всеки потребител или профил има списък от обекти, за които има права за достъп. Базите данни съдържат информация за потребителите и съответните приложения до които имат достъп, както и правилата за това какво могат да правят потребителите с даденото приложение.

3.21. Криптографски средства; Дефиниране на понятието криптография; Основни понятия при криптографията

Представката "крипто" ("crypto") идва от гръцката дума "krypto", която означава "скрит". Думата „криптология" („cryptology") идва от "кгуро" и "logos" и следователно означава "скрит свят". Тя се използва за описание на изследователските области в криптографията и криптоанализите. Древните гърци са използвали тази дисциплина за скриване на информация. Криптографията е изкуство дадена информация да се запази конфиденциална, в такава форма, в която не може да се прочете от човек, който не притежава необходимия ключ. Криптоанализите са изкуството да се използват алгоритмите разработени в криптографията.

Криптирането може да се използва за нещо повече от конфиденциална комуникация. Посредством криптиране могат да се трансформират данни във форма, от която те не могат да се четат без четящия ги да има подходящо „познание" за схемата на криптиране. Това „познание" се нарича ключ. Ключът се използва за разрешаване на контролиран достъп до информацията на определени хора. При това положение информацията може да се изпрати до всеки, но само тези, които имат правилния ключ могат да я видят.

Често се приема, че криптирането е компонент на сигурността, но в действителност то е механизъм за постигане на сигурност.

- ***Основни понятия при криптографията***

Ключ - променлива стойност, която се прилага в алгоритмите за получаването на кодиран текст от некодиран или от блокове от некодиран. От дължината на ключа зависи доколко трудно ще бъде разкодирането на текста в кодираното съобщение.

Частен ключ - частен ключ или секретен ключ е кодиращ/декодиращ ключ, известен само на едната страна от тези, които разменят кодирани съобщения. Традиционно в криптографията трябва да има ключ, който да е достъпен и за двете страни така, че всеки да може да кодира и декодира съобщения. Рискът при такава система е, че ако ключът бъде разбит или откраднат, системата спира да бъде защитена (на практика тя е разбита). В такива ситуации частния ключ се използва заедно с публичен ключ.

Публичен ключ - стойност, която комбинирана по подходящ начин с частен ключ може да се използва ефективно за декриптиране на кодирано съобщение и електронен подпис. Използването на публичен и частен ключ е известно като асиметрична криптография.

Криптиране - преобразуването на информация във формат, който не може да бъде разбран лесно от неоторизирани хора. Декодирането е обратната трансформация - от кодиран в разбираем формат. Има прости алгоритми за криптиране, които само разменят местата на буквите с цифри, а по-сложните методи, които се основават на "интелигентни" алгоритми - трансформират информацията в цифров вид и ако желаете да възстановите съдържанието на кодираното съобщение се нуждаете от декодиращ ключ.

Кодирането/декодирането е много често приложимо когато се пренася информация с голяма важност (когато се извършват покупки online, или при конферентна връзка между служители на фирма, обсъждащи строго секретни теми). Колкото по-добре е генериран криптиращия ключ, толкова по-надеждно е кодирането и толкова по-трудно е за неоторизирани лица да разшифроват информацията. В наши дни методите на кодиране се развиват с доста бързи темпове и това рефлектира върху ключовете (криптиращ и декриптиращ). На практика при наличието на единия от двата ключа е практически невъзможно да се открие другия, а при кодирани данни те не могат да се разкодират без наличието на декодиращ ключ.

SSL card (Server Accelerator Card) е PCI компонент, който се използва за генериране на кодиращи ключове за сигурността при транзакциите в Web сайтовете за електронна търговия. Когато транзакцията е започнала, сървъра на Web сайта изпраща информация до клиентската машина. По този начин става проверка на идентификацията на Web сайта. След тази размяна кодиращия ключ се използва за кодиране на всичката информация, която се трансферира между двете страни така, че цялата лична и всякаква друга информация (например за кредитна карта) е защитена. Този процес чувствително намалява производителността на

сървъра (могат да се извършва само по няколко транзакции в секунда) и именно тук на помощ идва SSL card. Процеса по размяната на информация се поема от картата и така сървъра се "облекчава", по този начин се повишава ефективността му. SSL card поддържа няколко протокола за сигурност (SSL - Secure Sockets Layer, SET - Secure Electronic Transaction и др.). Картата се инсталира на PCI слот на сървъра, стартира се драйвер който да я управлява и сървъра е готов да приема заявки. Този начин е много по-лесен и много по-евтин отколкото да се закупуват допълнителни сървъри. Съществува възможност за добавянето на още SSL card на сървър, на който има вече инсталирана такава. Същетвуват и други уреди, които изпълняват роля подобна на SSL card (SSL accelerators). Това са външни модули, които имат интегрирани карти. Тези устройства се вграждат в сървърите и когато се установи започването на транзакция, управлението се пренасочва към SSL accelerator-а.

- ***Причини за използване на криптиране***

Криптирането позволява изпращане по електронна поща на конфиденциални данни, като договори или персонална информация, или съхраняване на конфиденциална информация върху преносим компютър, без да има опасения, че някой може да я открадне и данните да бъдат разпространени. Без сериозно криптиране всяка информация може да бъде прихваната лесно и използвана срещу нейния притежател. Пример за това може да бъде отдела за покупки на дадена компания, който комуникира с доставчиците, или компания, която разменя ценови листи, договори, спецификации и информация за нови продукти със своите партньори.

Бизнес компаниите разменят все повече и повече информация през Интернет. В много случаи тази информация е с финансов произход и в случай, че попадне при друг получател, може да има негативно влияние върху бизнеса на компанията. За целите на електронния бизнес, информацията трябва да се запази конфиденциална. Без използването на криптографски методи, това не може да се гарантира.

Най-важното приложение, което трябва да използва криптиране е електронната поща. Без криптиране, електронните пощи са електронен еквивалент на класически пощенски картички. Електронните пощи нямат физическа форма и могат да съществуват електронно на повече от едно място в един и същи момент от време. В случай, че имате инсталиран добър софтуер за криптиране и декриптиране, той автоматично ще криптира изпращаните от вас съобщение и ще декриптира получаваните. Всичко, което трябва да направите е да посочите, че дадено съобщение трябва да бъде криптирано. Криптираните електронни пощи могат да се отъждествят с писмо, което е запечатано в плик и поставено на сигурно място. Тези, които не притежават ключа не могат да видят съдържанието.

С увеличаването на броя на използваните компютри и мрежи, въпроса за гарантиране сигурността на информацията предавана през мрежите става все по-важен. Поради факта, че компютърния свят премина от структурирани системи към среда клиент/сървър, криптографията започна да се превръща във фундаментално бизнес средство. Интернет, която е база за много бизнес транзакции, понастоящем е несигурна, тъй като всеки може да прихване дадено предаване. Въпросите със сигурността в Интернет се решават бавно, защото промяната на фундаменталните стандарти е трудна.

Онлайн банките и онлайн плащанията са двете най-големи Интернет приложения, които разчитат на криптирането. Интернет клиентите са много чувствителни на тема сигурност. Поради тази причина, всички web браузъри поддържат криптиране на документите. Стандартната дължина на ключа при международните версии на браузърите е 40 бита. Поради факта, че тази дължина е малка, декриптирането на ключа е лесно и в много случаи се налага използването на допълнителни компоненти за криптиране.

С криптографията може да се изпълни и контрол на достъпа. Телевизионните канали, които са достъпни само за абонати работят на този принцип. Поради факта, че не е възможно да се отварят или затварят канали за индивидуални абонати през сателит, информацията се криптира и ключа се разпространява към тези, които са платили за тези канали. В зависимост от типа на телевизионния канал ключа е валиден за цял ден, или се променя за всяка програма. В последният случай, ключа за определена програма се разпространява до клиентите, които са платили за нея. Ключовете се съхраняват в приемник, който декодира

програмата. Приемникът е свързан към доставчика по телефонна линия, по която може да се изпрати или отнеме ключа.

- ***Криптиране със секретен ключ***

Това е класическия вид криптография, наричана още симетрична. При нея се използва един единствен ключ за криптиране и декриптиране. Двете страни включени в обмена на информация, трябва да се споразумеят за ключа преди обмена. Ключът не трябва да се предава през същата среда, през която се предава криптираното съобщение. В случай, че изпратите криптирано съобщение по Интернет, добре е да се уточните за ключа по телефона.

Паролата (или ключа) се използват за криптиране на изходящи съобщения. Така наречения шифриран текст се изпраща по мрежата и получателя декриптира входящите съобщения с използването на същия ключ. Някои от алгоритмите са базирани на математически изчисления. Тези системи не могат да бъдат разкодирани от друг алгоритъм. Единствения начин за тяхното разкодиране е като се изпробват всички възможни ключове. През януари 1999, едно криптирано съобщение с 56 бита беше разкодирано за 24 часа от фондацията Electronic Frontier Foundation(www.eff.org). Понастоящем времето за разкодиране на криптирани съобщения при отсъствие на ключ на-малява значително.

Все още криптирането с обществен ключ има някои предимства. То е по-бързо и изисква ключа да се състои от по-малко битове, при което се получава същата степен на защита. Най-често използваните техники за ключове са блоковите и непрекъснатите шифри.

Непрекъснатите шифри са известни със своята бързина. Тя се постига чрез работа върху малки части от обикновения текст. Обикновено тези шифри работят на ниво битове. Така наречения непрекъснат ключ, който се състои от последователност от битове използва операция изключващо ИЛИ. Защитата на даден бит зависи от предходните битове.

От друга страна, блоковия шифър трансформира блок от обикновен текст с предварително определена големина (например 64 бита) блок от шифрован текст със същата големина. Трансформацията с прави чрез предоставяне на секретен ключ, който се използва за криптирането. Декриптирането става по същия начин, като към шифрования текст се приложи същия секретен ключ. Този тип криптография се използва например при среди с един потребител. В случай, че искате да криптирате своите файлове на твърд диск, няма смисъл да използвате криптиране с обществен ключ, тъй като то ще бъде по-бавно, а и освен това съхраняването на обществени и частни ключове в една среда няма никакво предимство пред използването на един ключ.

- ***Криптиране с обществен ключ***

Криптирането с обществен ключ или още така нареченото асиметрично криптиране има едно основно предимство пред симетричните алгоритми - то не разчита на защитен способ за размяна на парола. Симетричните алгоритми изискват двете страни да се споразумеят за общ ключ, който може да се прихване при предаване на информацията от единия на другия участник. Това прави криптирането в Интернет безполезно, щом като изпращате ключа преди да изпратите криптираното съобщение. Ключът трябва да се изпрати отделно, но това не позволява компании, които не се познават да имат бизнес отношения през Интернет.

През 1976 г. двама професори от Университета в Стафорд - Уитфилд Дифъл и Мартин Хелман предложиха система, която нарекоха „криптиране с обществен ключ". При този тип криптиране се използват два ключа за всяко криптиране и то може да работи добре при мрежите, в които отсъства защита. Всеки от ключовете представлява голямо цяло число. Двата ключа са свързани един с друг и с помощта на специални изчисления е възможно с помощта на единия ключ да се криптира съобщение, а с помощта на другия да се декриптира. В този случай не може да декриптирате съобщението с ключа, с който сте го криптирали.

През 1975 г. трима изследователи в MIT разработиха алгоритъм за реализация на криптирането с обществен ключ - те измислиха системата RSA, която носи имената на тримата и изобретатели.

Алгоритъмът RSA генерира първоначално два различни ключа за всеки потребител. Единият от тези два ключа се определя като обществен. Последният може да се

разпространява свободно. Общественият ключ не може да се използва за декриптиране на съобщение - той може да се използва само за криптиране на съобщения изпратени до собственика на ключа. Само този, който притежава другия ключ, така наречения персонален ключ, може да декриптира съобщенията, които са криптирани с обществения ключ.

Безспорно много математици са се опитвали да блокират алгоритъма на обществения ключ, като са правили различни изчисления, но до момента никой не е намерил алгоритъм, който да реши математическия проблем. Програмите за декриптиране се опитват да „разрушат" ключа, но до момента това не е станало. Въпреки, че всичко това не е невъзможно, от гледна точка на изчисления, то е неуместно, тъй като обществения ключ е прекалено дълъг.

В повечето случаи за криптиране на съобщения не се използва RSA, защото при нея изчисленията отнемат дълго време. За повечето съобщения продължителното време за криптиране и декриптиране е неприемливо. RSA се използва за криптиране на симетричен ключ, който криптира самото съобщение. Стандартът SSL, който се използва за криптиране на web страници (URLs използва https:// вместо http://) използва именно това свойство. Ключът се генерира в web браузъра и след това се изпраща към web сървъра. В случай, че не се използва криптирането с общ ключ, ключа трябва да се изпраща през Интернет без да е защитен.

За да се направи предаването на ключа сигурно, web сървъра изпраща своя общ ключ към web браузъра. Последният избира симетричен ключ и криптира съобщението с обществения ключ на web сървъра и го връща обратно. Web сървърът е единствения, който може да декриптира обществения ключ със своя персонален ключ. RSA ключът се използва като плик за симетричния ключ. От този момент нататък криптирането се прави със симетричен ключ, тъй като то е по-бързо от криптирането с общ ключ.

При тази система симетричните ключове могат да се избират произволно. В случай, че някой може да разкодира едно криптирано съобщение, няма да получи никаква информация за ключовете, използвани при останалите съобщения.

В случай, че решите да криптирате електронни пощи, можете да криптирате симетричния ключ няколко пъти с различни обществени ключове. Всеки общ ключ принадлежи на един получател. При това положение всеки получател може да декриптира съобщението. Всеки общ ключ формира плик, който съдържа същия ключ за декриптиране на оригиналното съобщение. Тази парадигма за гарантиране на защита се използва, например при PGP и по подобен начин се използва при SSL криптирането при web.

- ***Сравнение между криптирането със секретен и общ ключ***

Основното предимство на криптирането с общ ключ пред това със секретен ключ е, че персоналните ключове никога не се предават. Това прави този тип криптография по-сигурна и удобна. В една система със секретен ключ, е необходимо предаване на ключовете, което е свързано с рискове. Освен това при работа със секретни ключове механизма на идентифициране се осъществява трудно. Когато един цифров подпис използва инфраструктура с общ ключ се налага предаване на секретна информация. За да се избегне отказ на плащане се налага трета страна да проверява идентичността.

Безспорно криптирането с общ ключ има няколко недостатъка. Повечето технологии на секретни ключове са по-бързи от алгоритмите за криптиране с общ ключ. Тъй като бързината е по голяма с порядъци, криптирането с общ ключ не е препоръчително да се използва за големи файлове. За да може една система да бъде и защитена и бърза, е необходимо да се комбинират и двата типа криптография.

При такава комбинация съобщението ще се криптира със секретен ключ, защото при криптиране с общ ключ ще се отнеме много време, а секретния ключ се прикрепва към съобщението, като самия секретен ключ е криптиран с общ ключ. По този начин се постига и по-висока скорост и защита.

При SSL криптирането, което се използва за сигурен обмен на информация през web, криптирането с общ ключ се използва за размяна на секретния ключ. Web сървърът изпраща своя общ ключ към web браузъра. Последният създава ключ на сесия и криптира ключа на сесия с обществения ключ на web сървъра. След това ключа на сесия се

предава обратно на web сървъра, който го декриптира с помощта на своя секретен ключ. По този начин ключовете на сесии могат спокойно да се предават през незащитени мрежи. След като ключа на сесия се предаде, той се използва за криптиране на връзката, тъй като е доста по-бърз. Алгоритмите за секретните ключове ще бъдат от значение до момента, в който компютрите не станат поне хиляди пъти по-бързи от съвременните компютри. Ключът на сесия е сигурен, защото е валиден само за една определена сесия и след това не може да се използва повече.

- ***Криптографски метод Steganography***

Съобщенията, които са криптирани посредством метода Steganography, изглеждат като безвредни съобщения с прикрепени изображения или файлове със звук. Тези, които се опитат да прихванат такъв файл, ще получат съобщение и ще останат с впечатление, че то не съдържа секретна информация. Някой, който чете такава поща, разглежда изображение или чуе звук никога няма да забележи разликата. В повечето случаи скритите съобщения също са криптирани, при което се забелязват още по-трудно. Софтуерът използван при този метод се опитва да скрие информацията в обикновени звуци и изображения. За да останат незабелязани, скритите съобщения трябва да имат същата статистика, както тази на обикновените изображения и звуци. Проблемът е в това, че криптираните съобщения обикновено изглеждат по-различни от тези, които се стремят да имитират. Компютърно-генерираните изображения не са добро място, в което може да се скрие информация, защото са съвсем традиционни, докато едно сканирано изображение предлага повече възможности. Съществуват софтуерни пакети, които се разпространяват безплатно и позволяват криптиране от този тип. За съжаление обаче качеството не е добро. В случай, че внимателно анализирате данните, лесно ще откриете скритото съобщение. Често симулацията на естествен звук не е надежден начин за скриване на информация.

Комерсиалните софтуерни пакети използвани за този тип криптография предлагат по-качествено скриване. С използването на тази техника е възможно предаване на данни без никой да забележи това. В страните, където криптирането е забранено се използва именно тази техника. Изпращането на изображения през Интернет не е нещо необичайно и проверката за това дали съдържат криптирани или скрити съобщения е доста трудна, ако не и невъзможна.

- ***Приложения за криптиране***

Налагане на конфиденциалност

В Интернет, конфиденциалността е един от най-важните въпроси. По подразбиране Интернет е незащитена среда, и всеки може да прихваща съобщения, разменяни между две страни. Конфиденциалността на предаваните съобщения може да се обезпечи посредством тяхното криптиране, при което трети лица не могат да ги четат. Все още е възможно прихващането на съобщения, от където следва, че е необходимо да се гарантира, че ключовете не се предават през Интернет като прозрачен текст.

Конфиденциалността не е единствения важен въпрос при Интернет. От съществено значение е сигурността на мулти-потребителските системи, като сървъри, където няколко потребителя могат да споделят един и същи диск или конфиденциална информация. Файловете се защитават посредством пароли, което налага обезпечаване сигурността на паролите. Това може да се постигне като се съхрани не самата парола, а нейната hash стойност. Декодирането на паролите е възможно, но hash стойностите не могат да се променят. При въвеждане на парола от страна на потребител, hash стойността се изчислява и се сравнява със съхранената. При това положение не е възможно да се „крадат" данни, съхранени на система, чиято парола не се знае.

- ***Криптиране на електронна поща***

Електронната поща е най-използваното нещо в кибер пространството. Тя се използва много лесно и не изисква нищо освен компютър, връзка към Интернет и елементарна програма за изпращане и получаване на електронна поща. Съдържанието на електронната поща е във форма на обикновен текст и може да се прочете на всяка компютърна система.

Простотата на приложението обаче е проблем, защото при предаването му всеки едни компютър по света може да го прихване и да се прочете съдържанието без да се налага използването на допълнителен софтуер.

При изпращане на електронна поща, тя не се предава директно към получателя и, а минава през определени компютри. Това намалява значително разходите за предаване на информацията, тъй като всеки компютър трябва да предаде информацията само до следващия. Пътят между източника и получателя се определя след изпращане на пощата, и например една поща от Щутгарт до Оксфорд може да премине през компютри в САЩ. Всеки един от компютрите, участващи в предаването може лесно да провери за определени изпращачи и получатели и може да запише цялата информация от съобщението във файл на локалния си твърд диск. Дори ако атакуващия не стои на някой от компютрите, участващи в предаването той може да филтрира потока от съобщения и да получи необходимата информация. Нападението изисква от хакера да инсталира определен софтуер на съответния компютър. Този софтуер се нарича „прихващач". Последният сканира всички електронни пощи за това дали съдържат определени ключови думи.

Нормално изпращането на електронна поща до всяко едно място по света става за няколко секунди. Никой няма да забележи, ако някой вземе някаква информация, дори никой няма да забележи, че дадена информация е променена преди да бъде изпратена, тъй като няма определено време, за което да се получават съобщенията. Всички останали електронни пощи с изключение на класическите, нямат плик, който да скрива изпращаната информация. Електронните пощи са по-лоши от пощенските картички от гледна точка на конфиденциалност. Електронните пощи предавани през Интернет могат да бъдат сканирани за ключови думи лесно и автоматично. Сканирането на нормална поща в офиса ще изиска доста време, което прави процеса на сканиране непрактичен.

Криптирането на електронна поща може да стане по няколко начина. Най-сигурната система за криптиране, която понастоящем се намира на пазара е PGP. Системата PGP изисква инсталиране на отделен софтуер.

От друга страна софтуера S/MIME (Secure Multipurpose Internet Extensions) е доста по-прост за настройка, тъй като той се поддържа от Netscape Communicator и Internet Explorer. За използването на S/MIME не се изисква никакъв друг софтуер. Единственото нещо, от което имате нужда е цифров сертификат, който може да получите от много места, като TrustCenter (www.trustcenter.de) или GTE (www.gte.com) Софтуерът S/MIME използва подобен на PGP метод. Той използва асиметрично криптиране като плик, в който се изпраща ключ използван в симетричен шифър, който криптира съобщението. Софтуерът S/MIME гарантира по-малка сигурност от PGP, тъй като използва по-малък брой битове за ключове извън САЩ й изходния код не беше открит, до момента когато Netscape отвори Mozilla web сайта и представи кода за своя браузър.

Друг начин за криптиране на съобщение е използването на алгоритми за симетрично криптиране, които не са свързани със софтуера за електронна поща. Може да напишете своята поща с текстов редактор, да я криптирате и след това да я изпратите през мрежата. Може да избирате между Blowfish, IDEA и triple-DES. Само че на всички компютри трябва да е инсталиран софтуер за декриптиране на файловете и трябва да е установен канал за сигурен обмен на ключовете. Процедурата за инсталиране, поддръжка и използване на този метод е прекалено дълга, за да може да се прилага в бизнес среди. Методът е добър за персонално използване.

В случай, че ви е необходимо секретно предаване на информацията по такъв начин, че да може предаваната информация да се чете от повече от един получател, може да използвате програми като WinZip (www.winzip.com). Почти всеки има копие и може да го използва лесно. Освен това технологията за криптиране, която се използва е доста добра, файловете са защитени с парола, която може да се разбере, но вие можете да променяте паролата всеки път. Освен това паролата може да се предава и по телефона.

- ***Прилагане на технологиите за криптиране***

Има много и различни типове и видове нива на сигурност. Някои от тях, като например ROT13, се разбиват много лесно, други като PGP (www.pgp.com) не могат да бъдат

разрушавани в рамките на приемливо време. Реално действието им се прекъсва като се използват няколко хиляди компютъра в продължение на няколко хиляди години. Това, което трябва да имате при работа с тези алгоритми е парола и ключ за декриптиране, който се изпраща в PGP формат.

Сигурността и конфиденциалността са много важни за вашата компания въпроси, и един малък бъг в софтуера за криптиране може да доведе до много по-големи проблеми, отколкото бъг в текстообработваща програма.

- ***Степени на криптиране***

Технологиите за криптиране могат да се разделят в няколко групи, в зависимост от степента на защита/ криптиране:

Слаби - Такива са текстовите документи, защитени с парола от текстообработваща програма. Този тип програми използват криптиране с много ниска степен и с помощта на прости средства може да се разбере използваната парола;

Устойчиви - С използването на технология за симетрично криптиране може да се създаде устойчива защита, но слабата страна на тези технологии е в това, че при предаване на ключа през несигурни мрежи той може да се прихване;

Силни - С използването на технология с обществен ключ, предаването на ключа през несигурни мрежи е безопасно;

Такива са One-Time Pads. Този тип система използва ключ, чиято дължина е колкото дължината на съобщението и който не може да бъде декриптиран със средствата, с които е извършено криптирането.

Един бъг в софтуер или хардуер за криптиране може да повлияе негативно на целия ви бизнес, просто защото всички конфиденциални неща на вашата компания ще бъдат достъпни за всекиго. Повечето текстообработващи програми предлагат възможности за криптиране на документи, но алгоритмите за криптиране са много слаби и никога не трябва да разчитате на тях. Те могат да се използват да скривате данни намиращи се на сървъра от колеги, но в никакъв случай няма да представляват пречка за професионалисти. Компанията AccessData (www.accessdata.com) дори е създала софтуерен пакет, който е специализиран за разбиването на кодове на такива програми. Този софтуер се продава, за да може когато някой забрави паролата си да я възстанови, но разбира се софтуера може да се използва и за недобронамерени цели.

Друг популярен метод за защита на документи е просто да ги скриете. Сигурността посредством неяснота е доста слаб метод на защита. В действителност той е дори по-лош от криптиране с текстообработваща програма. С поставянето на документи на неправилно място, някои хора си мислят, че могат да ги скрият от останалите, но в действителност всеки може да ги намери. С използването на обикновено търсене на файл, в повечето случаи се постига желания резултат. Дори и при използването на слаба защита е необходимо време за декриптиране.

Файловете криптирани със силна защита могат да се оставят на обществени сайтове без да имате опасения, че някой може да прочете съдържащата се в тях информация, дори и ако ги открадне. Дори и алгоритмите и изходния код на повечето популярни технологии за криптиране да са налице, никой не може да разбере какъв е принципа на криптиране. Сигурността идва от алгоритмите, а не от системата, която се използва за изпълнение на тези алгоритми. В случай, че ключа не се разпространява, никой не може да проникне в информацията.

3.22.Цифрови подписи; Модерен поглед върху електронния подпис

Освен за криптиране и декриптиране на информацията, криптографията може да се използва и за други неща. Идентифицирането е една от най-важните области при изграждането на връзка на доверие. Логично е, че можете да имате доверие на някой, само ако знаете кой е той. В много случаи идентифицирането се прави чрез подписване на документ. За да направите електронните документи легални трябва да имате механизъм, който да осигурява средство за идентифициране автора на документа.

За да направите една система приложима за цифров бизнес е необходимо само една малка част от съобщението да се криптира с персонален ключ. Тази част се нарича digital hash. Hash кода е функция, която намалява всяко едно съобщение до фиксиран брой битове. Без значение каква е дължината на файла, дължината на hash винаги е една и съща. Същността се крие в това, че hash кода е различен за всяка електронна поща.

Hash функцията е еднопосочна. Не е възможно да създадете определен код и да намерите съобщение, което да съответства точно на този код. Hash кода може да се разглежда като печат върху плик. Изпращането на този код заедно с електронна поща ще гарантира, че никой не може да промени съдържанието на пощата по време на предаване, но това не ви дава възможност да сте сигурни в изпращача. Поради факта, че този код е с фиксирана дължина, времето за неговото криптиране винаги е едно и също.

Цифровите подписи използват технологии за криптиране с обществен ключ, като RSA, но не работят като стандартното криптиране. Вместо да критпират съобщението с обществения ключ на получателя, hash кода на съобщението се криптира с персонален ключ, и след това се декриптира с обществения ключ на изпращача. Разбира се, всеки може да декриптира hash кода на съобщението, тъй като обществения ключ може да се намери в директорията за обществени ключове на сървъра. Само че факта, че вие можете да декриптирате hash на съобщението с обществения ключ на определен човек доказва само по себе си, че това съобщение идва точно от този човек. Само този, който притежава персоналния ключ може да създаде съобщение, което може да се декриптира със съответния обществен ключ.

При цифровите подписи има две причини за използването на hash код. Едната причина е, че криптирането на цяло съобщение само за целите на подписа отнема дълго време. Втората причина е, че всеки иска да криптира подписани съобщения. В много случаи дадено съобщение е предназначено за много хора, но автора му иска да докаже неговата идентичност.

За да може едно съобщение да се криптира сигурно и в същото време да има подпис, обикновено пощата се криптира с персонален ключ, а след това съобщението се криптира с обществения ключ на получателя, за да може всеки да вижда съдържанието.

Цифровият подпис свързва даден документ с притежателя на определен ключ, но често това не е добре, ако не се знае момента на подписването. Например, един договор, който е подписан с цифров подпис не е валиден, ако на него няма дата. Една онлайн покупка на намалена цена, която е валидна за определен период от време изисква да има посочена дата, за да се докаже, че продуктите са закупени в определения период.

От тук се вижда, че цифровия печат за дата е необходим за определяне момента на поставяне на цифровия подпис. Това може да се направи с добавяне на дата и час на документа от трета страна и след това тази информация се криптира с персонален ключ на третата страна. Цифровият печат за време свързва даден документ с момента на неговото създаване. Тази система не може да се използва на световно ниво, защото няма никакви регулатори, които да гарантират, че даден печат за време е валиден.

Не би трябвало да ни изненадва, че стандарта XML се е наложил вече и в тази област. От известно време съществува и спецификация за електронен подпис под формата на XML документ. В този документ се описват всичките важни характеристики на подписа. Така когато един документ се разпространява в Интернет, към него може да се прикрепи друг документ, с който да се удостовери валидността на първия. Следва един кратък пример за това как изглежда XML варианта на електронния подпис или както се нарича - XML Signature:

Пример:

```
<Signature Id="MyFirstSignature" xmlns="http://www.w3.org/2000/09/xmldsigtf">
   <SignedInfo>
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xroldsig#dsa-s;ial"/>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-cl4n-
20010315"/>
      <Reference URI="http://www.w3.org/TR/2000/REC-xhtmll-20000126/">
         <Transforms>
```

<Transform Algorithm«"http://www.w3.org/TR/2001/REC-xml-clIn-20010315"/>
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsigflshal"/>
<DigestValue>j61wx3rvEPOOvKtMup4NbeVu8nt=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>MCOCFFrVLtRlk=. . .<:/SignatureValue>
<KeyInfo>
<KeyValue>
<DSAKeyValue><P>. . .</P><0>. . .</QXG>. . .</GXY>. . .</Y></DSAKeyValue>
</KeyValue>
</KeyInfo>
</Signature>

3.23.Конфиденциалност в Интернет - Следи в мрежата

В Интернет анонимността е изключена по подразбиране. Всеки, който е в онлайн режим оставя ясни следи. Много потребители обаче не знаят този факт. Всеки web сайт може да създаде персонален профил на потребителя, без да се налага намеса от страна на потребителя. Маркетинг отделите на компаниите използват Интернет за да проследяват предпочитанията на клиентите.

Понастоящем повечето компании имат обявена политика на конфиденциалност на своята web страница и предупреждават посетителите, по какъв начин ще използват получена от тях информация. Онлайн бизнеса има нужда от събиране на информация с цел увеличава не продажбите на предлаганите продукти и услуги. Някои от компаниите, които реализират онлайн бизнес не казват на клиентите за какво им е необходима информацията, която изискват от тях и просто събират тази информация и предлагат профилите на други организации.

С помощта на Интернет за клиентите може да бъде получена значителна информация. При всяка заявка за нова web страница, името на браузъра; операционната система; предпочитания език, на който да се покаже страницата; информация за момента за последно посещение на web сайта; IP адреса и името на домейна на дадения компютър се изпращат автоматично към сървъра. С помощта на JavaScript, сървъра има възможност да получи повече информация за компютъра на клиента, като например резолюция и брой цветове на екрана.

Тази информация се изпраща обратно на сървъра и повечето хора не могат да спрат това изпращане. Възможно е да се изключи опцията JavaScript, но въпреки това, отново се изпраща доста информация. Въпреки, че всяка информация, която се изпраща сама по себе си по никакъв начин не нарушава вашата конфиденциалност, като цяло събраната информация може да има негативно влияние върху компанията. По името на домейна може да се разбере в коя част на света се намира компанията, а по използваните браузър и операционна система може да се правят изводи какъв е клиента. Цялата тази информация може да се използва за насочване на клиентите към онлайн офертите, но в същото време тя може да се използва за получаване на допълнителна информация.

При акумулиране на информация за даден клиент, често се използват cookies. Последните представляват файлове, които се съхраняват на компютъра на клиента и съдържат специфична информация, която може да се върне към собственика на сайта. Един cookie файл може да съдържа информация за паролата, необходима за определен web сайт, име на потребител, адрес на електронна поща или информация за покупки. Дизайнът на cookie файла не позволява разпространяването на информацията към други web сайтове, но има cookie-файлове създавани в миналото, от които може да се извлича информация. Друг проблем е

общата сигурност на операционната система на компютъра на клиента, която дава възможност на хакерите да откраднат файла „cookie.txt" без да оставят следи.

Популярните ICQ програми и техните UNIX предшественици „finger" ви позволяват да получавате персонална информация за собственика на определен адрес на електронна поща. Освен това, тези програми дават възможност да се види кога потребителя е прочел за последен път дадена поща и дали в момента този потребител е в онлайн режим. UNIX програмата Finger няма централизирана база данни, докато ICQ съхранява цялата информация за потребителите на едно централно място. За да използва ICQ, даден потребител трябва да попълни форма с персонална информация, която е частично налична за други потребители в Интернет.

Когато клиентите използват онлайн услуги, те оставят информация за себе си, като например - име, пощенски адрес, телефонен номер и адрес на електронна поща. Тази информация се използва в случаите когато клиентите се връщат към дадения web сайт. Проблемът е, че тази информация трябва да се съхранява на сигурно място, така че никой друг да няма достъп до нея. Неправилните концепции и неправилните конфигурации на web сървърите в миналото предоставяха тази информация на всички и може да се допусне, че и в бъдеще ще има подобни случаи.

Информацията за клиентите става все по-значителна и необходима за онлайн бизнеса. Получаването на достъп до базата данни с клиентите на конкурентите дава възможност на дадена компания директно да се свърже с тях и да ги атакува със специални оферти. Освен това, базата данни с клиентите дава възможност да се прецени как работи дадена компания и кои нейни продукти се продават добре.

Друго средство за събиране на персонална информация за даден клиент е просто като му се предостави безплатен софтуер, безплатни шапки, фланелки и други подаръци, срещу които той предоставя информация за себе си. Съществува и специален тип нов безплатен софтуер, който показва реклами докато клиента го разглежда. Рекламите са персонализирани според профила на клиента. Пример за такава програма е Copernic 99 (www.copernic.com), която предлага едновременно откриване на няколко Интернет машини за търсене. Преди да изтегли софтуера, клиента трябва да попълни определена форма, която показва какви реклами ще му се показват в последствие.

Друг начин за събиране на информация за потребител е като се преглеждат нюз групи. Тези които изпращат съобщения на определени нюз групи посочват своя адрес на електронна поща и достатъчно персонална информация. Например, тези които изпращат съобщения до нюз групи за пътувания в Испания, най-вероятно са заинтересувани от пътувания в този регион. Тази информация се използва от специалисти, прихващащи електронните пощи и след това изпращащи на потребителите подходящи реклами.

По подразбиране Интернет е отворена система, която предоставя средства за получаване на конфиденциална информация. Въпреки, че персонализирането е нещо, с помощта на което се намаляват разходите за всяка задача, разкриването на конфиденциална информация също може да има негативно влияние върху вашия бизнес.

Много организации се борят за налагането на стандарти в Интернет, но поради факта, че Интернет не принадлежи на никого не е възможно налагането на стандарти. Новите стандарти се развиват бавно и трябва да имат редица предимства за потребителите, за да може да бъдат приети.

3.24.Сигурност на финансовата информация

Това е основната част от една ефективна бизнес система. Двете страни в един бизнес трябва да се познават или да могат да намерят достатъчно информация един за друг, за да са уверени, че другата страна не ги лъже. В допълнение на това трябва да имат надежден начин за разплащане и за предпазване на компютърните им системи от външни нападения - особено когато са част от мрежа.

Една от основните пречки пред широкото разпространение на електронната търговия е проблема със сигурността на финансовата информация, която се изпраща в мрежата при извършването на електронни плащания. Методите за сигурност винаги са били притеснение при изпращането на плащания. Но изпращането на пари по пощата е също толкова рисковано,

както и изпращането на чек. В повечето съвременни бизнес отношения се използват плащания с кредитна или дебитна карта. Съществува риск и при двете страни, когато се прави това. Продавача иска да е сигурен, че картата се използва легитимно. Купувача иска да е сигурен, че търговеца няма да я използва за сума по-голяма от договорената. Когато информацията се изпраща на разстояние - по пощата, факса, или електронната поща, сигурността на връзката винаги е грижа.

Въпреки че купувачите изпращат такава информация по пощата или факса, изпращането по Интернет винаги ги е притеснявало. Част от това притеснение е може би непознаването на посредника и колкото повече хора използват този начин без проблеми, той ще придобива популярност. В действителност Интернет технологиите технически могат да предоставят абсолютно сигурно предаване на информация, като използва криптиране и протоколи и те могат да премахнат повечето, ако не и всички проблеми, които биха възникнали при извършването на плащания по този начин.

Други проблеми възникват от вируси и хакери. Но пък съществуват множество програми, които сканират получената информация и предпазват от вируси. Системите често са подложени и на нападения от хакери. Защита срещу тях предлагат защитните стени (firewalls).

- ***Firewall***

Firewall-а е защитен механизъм. Може да се реализира по многобройни начини. Идеята на firewall-а е да позволи на локалните потребители да се възползват от всички услуги на локалната мрежа и някои Интернет услуги, но едновременно с това да контролира обмена на дании и достъпа отвън до локалните ресурси. Firewall-а постига сигурност, като изолира локалната мрежа от останалия Интернет свят. Трафикът трябва да бъде контролиран така,че всички опасности да бъдат засечени. Каква опасност, зависи от политиката на сигурност определена от хората, които осъществяват този защитен механизъм. Спомнете си седемте слоя на OSI модела. Инспектирането на пакетите може да се приложи на всяко ниво от модела, но най-често се прави в Application слоя и Network слоя, съответно чрез Application layer firewall и Network layer firewalls.

Обикновено Application layer firewalls се наричат Application Gateways или Proxies, а Network layer firewalls - филтриращи рутери или сканиращи рутери.

- ***Филтриращи Рутери***

Те освен че изпълняват функциите на рутер, филтрират пакетите и решават, още преди да извлекат информация от рутер таблицата, дали да пропуснат пакета по-нататък. Филтриращото решение се взима на базата на Access Control List. Access Control List-а съдържа информация как да се процедира с пакета според произхода му. Каква информация се използва за филтриране на въпросните пакети? IP address на подателя и получателя, портовете отново на подателя и получателя, типа на протокола и ACK bit (TCP header, този бит определя дали пакета е потвърждение за получен TCP пакет).

- ***Application layer firewall – Proxy***

Proxy означава оторизиран представител. Идеята на Proxy компонента е да не позволява директна TCP (UDP) връзка между клиент от локалната мрежа и Интернет сървър. Вместо това връзката е раздробена на две части. Proxy програмата играе ролята на посредник. Тя трябва да имплементира достатъчна част от клиентските и сървърните протоколи. За клиента изпълнява ролята на сървър, а за Интернет сървъра е в ролята на клиент. Предава всички данни от клиента, предназначени за сървъра и обратно, като е натоварена и със функции относно сигурността.

- ***SET***

SET стандарта е създаден изключително за защита на Интернет финансови транзакции, докато SSL е система за кодиране с общо предназначение, която може да се използва за защита преноса на произволен тип данни. SET комбинира съществуващите защитни технологии с PKI, използвайки цифрови сертификати, както за притежателите на кредитни

карти, така и за търговците. PKI се използва за проверка дали участника в транзакцията е този, за който се представя. Това е от особено значение, тъй като Интернет не осигурява стандартен механизъм за проверка идентичността на даден човек или институция. Чрез използването на PKI е възможно въвеждането на концепция за неотхвърляне (признаване) на Интернет-базираните транзакции. Купувачите, платили чрез SET не могат след това да оспорят плащането, твърдейки, че те не са извършили транзакцията - всички поръчки се подписват цифрово, а цифровия подпис не може да бъде фалшифициран. Освен това, PKI се използва за изпращане на кодирана информация по Интернет. Използването на строго кодиране дава възможност за предаване на транзакции с кредитни карти по публични мрежи, каквато е Интернет.

SET е създаден през 1996 г. от Visa и MasterCard и представлява един от водещите стандарти в плащанията чрез кредитни карти по Интернет. SET спецификациите включват:

Висока степен на защита - информацията за кредитните карти може да бъде предавана по обществени мрежи, тъй като се използва строго кодиране;

Непрозрачност - показва се само необходимата информация. Търговецът не вижда информацията от кредитната карта, а банката няма информация за направената поръчка;

Стандартизираност - SET стандарта дефинира всички необходими процеси - потока на транзакцията, формата на съобщенията, идентифицирането и алгоритмите за кодиране;

Неотхвърляне - SET стандарта дефинира PKI, която се използва за проверка на участниците в транзакцията и за кодиране/декодиране на обменяните съобщения. Участниците се идентифицират чрез своя цифров подпис, гарантиращ неотхвърляне на сделката.

SET е създаден да осигури конфиденциален начин за плащане и поръчване на стоки. Цялата информация в SET транзакциите се кодира. Интегритета на предаваните данни се осигурява чрез цифров hash код, който се прилага към всяко съобщение и дава възможност на получателя да провери дали съобщението не е било променено по време на преноса. Използването на цифрови сертификати дава възможност да се удостовери, че притежателя на картата е и нейния легитимен ползвател. Освен това стандарта включва и идентификация на търговеца пред неговата банка. SET протоколът не зависи от допълнителните защити по време на транспортиране. Което позволява използването на SSL в допълнение на SET защитата.

SET осигурява функции за зашита на личните данни. Които затрудняват получаването на информация за потребителя. Извежда се само необходимата за даден участник в транзакцията информация. Примерно, търговеца не бива да получава информация за кредитната карта на потребителя - тази информация се насочва директно към банката.

SET 2.0 въвежда допълнителни защитни функции чрез използването на смарт карти. Тези карти представляват кредитни карти с вграден допълнителен чип, съдържащ цифров сертификат, както и обществен и личен ключ на потребителя. Понастоящем такива чипове се използват само в дебитните карти.

Използвайки карта с чип, потребителите ще могат да ползват услугите на всяко SET съвместимо устройство, независимо дали това е компютър, телевизор или терминал. Допълнително предимство на тези карти е, че те са аналогични на използваните POS и ATM банкови терминали. Това опростява процедурите за обработка и поддръжка.

Съществуват най-различни начини за плащане чрез кредитна карта. Недостатъкът на тези решения е, че те са затворени и свързани към конкретен доставчик на услуги.

3.25. Безконтактни плащания

Когато стане въпрос за личните финанси, малцина са тези, които са склонни да поемат рискове. Тези опасения, съчетани със скептицизма към новите технологии и страха от Големия брат подхранват оживените спорове около въвеждането на RFID чиповете в кредитните карти. RFID, или радиочестотната идентификация, е технология, която според едни представлява сериозна опасност за сигурността на личните данни, а според други е пробив, който не само ще улесни потребителите, но и ще даде основа за разработка на иновативни продукти. Наскоро например бе оповестен съвместният проект на Citigroup, MasterCard Worldwide, Cingular Wireless и Nokia, който ще превърне мобилните телефони в кредитни карти, чрез които плащанията ще се извършват не с въвеждане на пин код, а само с доближаване на уреда до стандартно четящо устройство. За разлика от традиционните кредитни карти, снабдени с магнитна лента, безконтактните карти, базирани на RFID технологията, работят чрез микрочип и радио антена, което позволява предаване на информацията без физически контакт между картата и четящото устройство. Защитниците на нововъведението изтъкват, че то е особено полезно за търговски пунктове с висока интензивност на клиентския поток, като бензиностанции, вериги за бързо хранене и супермаркети. Според извършени изследвания, докато плащането в брой отнема средно 34 секунди, при традиционните карти с магнитна лента са необходими 25 секунди, а при тези с RFID чип – едва 15 секунди. [11]

Също така, удобството при транзакциите изглежда оказва влияние и на желанието на потребителите на пазаруват. Доклад, публикуван преди няколко години сочи, че инсталирането на устройство за четене на безконтактни кредитни карти води до покачване от един процент на броя покупки в даден търговски пункт, а средната похарчена сума от клиентите скача с 15 на сто. Издателите на безконтактни карти American Express, Visa и Mastercard са постигнали договорка да не изискват подпис на клиента при транзакции с RFID карти на стойност под 25 долара, което допълнително улеснява пазаруването и значително намалява опашките.

Други плюсове на новата технология са и че радиочестотните идентификатори могат да съдържат голямо количество информация, а четенето да се извършва без човешка намеса. Освен това, за разлика от магнитните ленти, чиповете са устойчиви на външни влияния като температурни промени, влага, химикали и др. Не случайно според последната прогноза на фирмата за маркетингови изследвания ABI, пазарът на RFID технологията ще достигне 5.3 милиарда долара през 2008 г. и въпреки световната финансова криза, ще продължи експанзивния си ръст и през следващите пет години. Въпреки всички предимства на безконтактните кредитни карти обаче, лобито против тях е особено силно, и сред противниците на въвеждането им са и известни личности като Ричард Сталман, създателят на подобната на Unix безплатна операционна система GNU и основател на Фондацията за свободен софтуер. Издателите на безконтактни кредитни карти твърдят, че използват най-сигурните стандарти за закодиране на информацията, което прави почти невъзможно някой крадец да получи достъп до личните ви данни.

Например, вместо да предава номера на картата ви, RFID чипът създава уникален номер за всяка транзакция. American Express казват, че използват 128 битово шифроване, а J. P. Morgan Chase твърдят, че картите им, наречени Blink, са защитени чрез най-високите стандарти за сигурност, разрешени от американското правителство. Въпреки това обаче, екип изследователи към лабораториите RSA Labs излязоха със скандален доклад, представен на конференция по информационна сигурност. Според учените, ако използвате безконтактна кредитна карта, всеки технически грамотен престъпник може да получи достъп до част от личните ви данни, като създаде устройство чрез широко достъпни компютърни и радио компоненти, като за целта ще изхарчи по-малко от 150 долара. Според експертите, провели тестове с двайсет карти на Visa, MasterCard и American Express, част от предаваната чрез RFID чипа информация, като например името на картодържателя, не е кодирана. Те твърдят, че близо 20 милиона от безконтактните кредитни карти, които в момента са в обръщение, са достъпни за този вид атаки.

Опасността от радиочестотната идентификационната технология се крие именно в основното й предимство – факта, че данните могат да бъдат разчетени от разстояние. Това

означава, че въоръжен със съответното устройство престъпник може да получи достъп до информацията на всичките кредитни карти, които държите в портфейла си, просто докато стои зад вас на опашката в супермаркета или се вози в градския транспорт. Параноята относно сигурността на данните, обоснована или не, е толкова силна, че в интернет лесно може да се намерят съвети как да облепите портфейла си с метално фолио, за да се защитите от кражба на личните си данни. За съжаление, точно толкова достъпна е и информацията как да сглобите четящо RFID устройство за едва 30 долара. В условията на финансова криза, потребителите и без това не са особено склонни да се натоварват с допълнителни дългове, а страхът относно сигурността на личните данни допълнително може да ограничи пласмента на безконтактните кредитни карти, въпреки оптимизма на производителите на RFID чипове. Според наскоро публикувано проучване на Auriemma Consulting Group (ACG), само три процента от потребителите са наясно с новата технология.

3.26.Радиочестотна идентификация – Принцип на действие; Компоненти; Софтуер

Радиочестотната идентификация (англ. RFID - Radio-Frequency IDentification) е един от методите за автоматична идентификация и събиране на данни, в този случай за автоматично дистанционно идентифициране на обекти чрез RF комуникация. RFID се ползва най-често за етикетиране и идентифициране на мобилни обекти, като стоки в магазин, пощенски пратки, маркиране на животни (например домашни любимци или при биологични изследвания) и позволява те да бъдат проследявани при движение от едно място на друго. RFID технологията включва комуникационна мрежа за локализация и идентификация и малки (често пъти по-малки от нокът) компоненти хардуер, наречени RFID микрочип, радио-имплант или идентификатор, които могат да се реализират като процесорен чип, като FPGA интегрална схема за кодиране на комуникации и др. [12]

RFID системите може да се ползват както за съхранение на данни и информация върху чип, така и като обикновени четци на данни. RFID системите са създадени като алтернатива на баркода (щрих-кода). В сравнение с щрих-кода, RFID идентификацията позволява обектите да бъдат сканирани от значително по-голямо разстояние, поддържа съхранение на данни и позволява проследяване на повече информация за даден обект.

- ***Принцип на действие***

Технологията е базирана на радиочестотна комуникация между специално изработен идентификатор (етикет, таг, карта, ключодържател, стикер и т.н.) и четящо устройство. Всеки идентификатор съдържа чип със записан уникален номер и антена. В зависимост от конфигурацията на системата при “прочитане” на номера може да се предприеме действие — например да бъде задействана врата, бариера или друго устройство — или информацията да бъде подадена към компютър. Някои типове RFID устройства позволяват многократен запис на информация, с което възможностите за тяхното използване допълнително се разширяват. Разстоянието, от което може да бъде “прочетен” идентификатора зависи от много фактори като честота, форма и размер на антените, околна среда и др. и може да достигне до десетки метри при използване на активни RFID идентификатори.

Често RFID идентификаторите са наричани баркодовете на 21 век, но това определение е доста непълно. Възможностите, които тази технология предлага, са несравнимо по-големи от тези на баркода:

- Информацията може да бъде ”четена” от разстояние и без пряка видимост (при внасянето на стоката в склада, директно на рафтове или поточни линии);
- Могат да бъдат идентифицирани голям брой стоки едновременно;
- Идентификаторите могат да съдържат по-голямо количество информация;
- Четенето може да се извършва без човешка намеса;
- Идентификаторите са устойчиви на външни влияния (температура, влага, химикали и др.);
- Възможен е многократен запис на информация през целия жизнен цикъл на изделието;

Една от глобалните инициативи в тази насока е EPC Global, обединяваща водещи фирми и целяща създаване на единна система за маркиране на всяка отделна стока, като информацията ще е достъпна през Интернет. Очевидно реализацията на този проект ще отнеме време, но подобни системи вече функционират в някои от най-големите световни търговски центрове като Wal-Mart, Metro, както и Министерство на отбраната на САЩ.

Независимо от различията в изпълнението, честотата и софтуера, всяка RFID система работи с определена работна честота.

- ***Работна честота***

Ниска честота — Low Frequency (LF)

Честоти между 30 и 300 kHz се приемат за ниски. Обикновено LF RFID системите функционират на 125 kHz, по-рядко – на 134 kHz. LF устройствата имат ниска скорост на обмен на данните между идентификатора и четеца, но са много устойчиви в близост до метал, течности, сняг и др. Стабилното поведение на тези устройства в неблагоприятна среда е много важна тяхна характеристика, способстваща за широкото им разпространение. LF системите, работещи на 125 kHz са най-разпространените в Европа (включително България), като системите за контрол на достъп са най-типичното им приложение.

Висока честота — High Frequency (HF)

Честоти между 3 и 30 MHz. Стандартната честота за HF RFID система е 13.56 MHz. Този тип системи са широко разпространени, като техните характеристики са регламентирани и от международните стандарти ISO 15693 и ISO 14443. Това дава широки перспективи пред използването на HF устройства в различни области и улеснява въвеждането на такива системи. Сред недостатъците е нестабилното поведение на 13.56 MHz идентификатори в близост до метал или течности, но това не е пречка за използването им в голям брой приложения за проследяване на стоки и материални активи, в библиотеки, в текстилната индустрия, за електронни разплащания и много други.

Ултра висока честота – Ultra High Frequency (UHF)

Честоти между 300 MHz и 1 GHz. Типичната честота за пасивна UHF система. В Европа е между 865.7 - 867.5 MHz, в САЩ: 902.75 - 927.75 MHz, в Тайланд: 922.25 - 927.75 MHz. Активните UHF системи функционират на 315 или 433 MHz. Бързият трансфер на данни и ниската цена на идентификаторите са важни предимства на UHF. Основният недостатък е зависимостта им от средата и най-вече смущенията в работата в присъствието на метали и течности.

Микровълнова честота

Честоти над 1 GHz. Стандартно се използват 2.45 или 5.8 GHz. Идентификаторите могат да бъдат с много малки размери, трансферът на данни е най-бърз в сравнение с другите честоти, но металите и течностите са сериозна пречка за използването на микровълновите системи.

- ***Компоненти***

Всяка RFID система се състои от следните компоненти:

Идентификатор

RFID идентификаторите притежават антена за предаване и получаване на радио-сигнали. Пасивните RFID чипове нямат собствено захранване, докато активните имат. RFID чиповете може да се прикрепят към обектите (етикет, таг, карта, ключодържател, стикер и т.н), като пасивните могат дори да бъдат инжектирани в обектите.

RFID идентификаторите могат да бъдат класифицирани по различни признаци:

Форма

- стандартна смарт карта (ISO 7816-1) с размери 86 x 54 x 0.76 mm;

- Clamshell карта с размери 86 x 54 x 1.8 mm;
- ключодържател – различни форми и размери;
- стикер;
- часовник;
- диск;
- стъклена ампула – за имплантиране под кожата на животни;
- дюбел, пирон и др.

Захранване

- пасивни – нямат вградено захранване (батерия). Простото им устройство ги прави много дълготрайни, с живот около 10 години, както и много устойчиви на външни условия (температура, влага, химикали и т.н.). Цената им е ниска, сравнена с другите видове идентификатори, но отстъпват по разстояние на четене.
- активни – имат собствено захранване, вградено в идентификатора. Това им позволява по-голямо разстояние на четене и възможност за вграждане на микропроцесор и извършване на допълнителни функции (измерване на температура, следене на определени параметри).
- полу-пасивни – имат захранване, подобно на активните идентификатори. Батерията подобрява дистанцията на четене. Някои от тях изчакват сигнал от четеца и така пестят живота на батерията.

Възможности за четене и запис

- само за четене, Read Only (RO) – в процеса на производството с помощта на лазер в чипа се записва уникален номер, който не може да бъде променян впоследствие. Имат широко приложение поради ниската си цена и простотата на използването им. При комуникация с четеца RO идентификаторите изпращат номера си, и така идентифицират преносителя си.
- еднократен запис, многократно четене, Write Once Read Many (WORM) – записът се извършва при първото използване на идентификатора. Имат добро съотношение цена/производителност, поради което имат широко разпространение за бизнес приложения.
- за четене и запис, Read Write (RW) – могат да бъдат презаписвани много пъти (10 – 100 000, дори и повече). Записът може да се извършва както от четеца, така и от самия идентификатор при използване на активен тип. Могат да бъдат използвани за много различни приложения, но разпространението им е ограничено от все още високата цена.

Четец

Системата ползва специално устройство, наречено „RFID четец“. Той е основен компонент на RFID системите, който комуникира с идентификатора и извършва четенето и записа. В различните приложения той може да съдържа в себе си антена, контролер, памет. За някои по-прости приложения, като контрол на достъп до жилищни сгради, асансьори, четецът може да е изпълнен като самостоятелно устройство, без връзка към компютър и софтуер. За мобилни приложения се използват ръчни терминали, често с допълнителни възможности на джобен компютър.

Винаги когато четецът сканира за обекти в своя работен обхват, той изпраща контролни сигнали до обекта, при което RFID чипът предава заявената информация, като напр. идентификационен номер и дата на производство на продукта (пасивните RFID чипове извличат енергията, необходима за изпращане на отговора, от входния сигнал). Четецът на свой ред извежда на дисплей така получените данни за разчитане от оператор или предава данните по-нататък на централизирана мрежова компютърна система.

Антена

Антената предава електромагнитен сигнал от четеца към идентификатора, който връща отговор към четеца. По този начин се изпраща и получава информация. Правилното разполагане и геометрия на антената са особено важни за разстоянието на четене. Размерите и видът на антените са свързани с работната честота на RFID системата. Често антената е интегрирана в четеца.

Контролер

Контролерът е модулът, позволяващ комуникация и контрол на четеца от компютър. Присъствието му в системите е задължително, ако е необходимо използване на информацията, прочетена от идентификаторите в компютърни системи. Контролерът предава инструкциите към идентификаторите и в случай на запис.

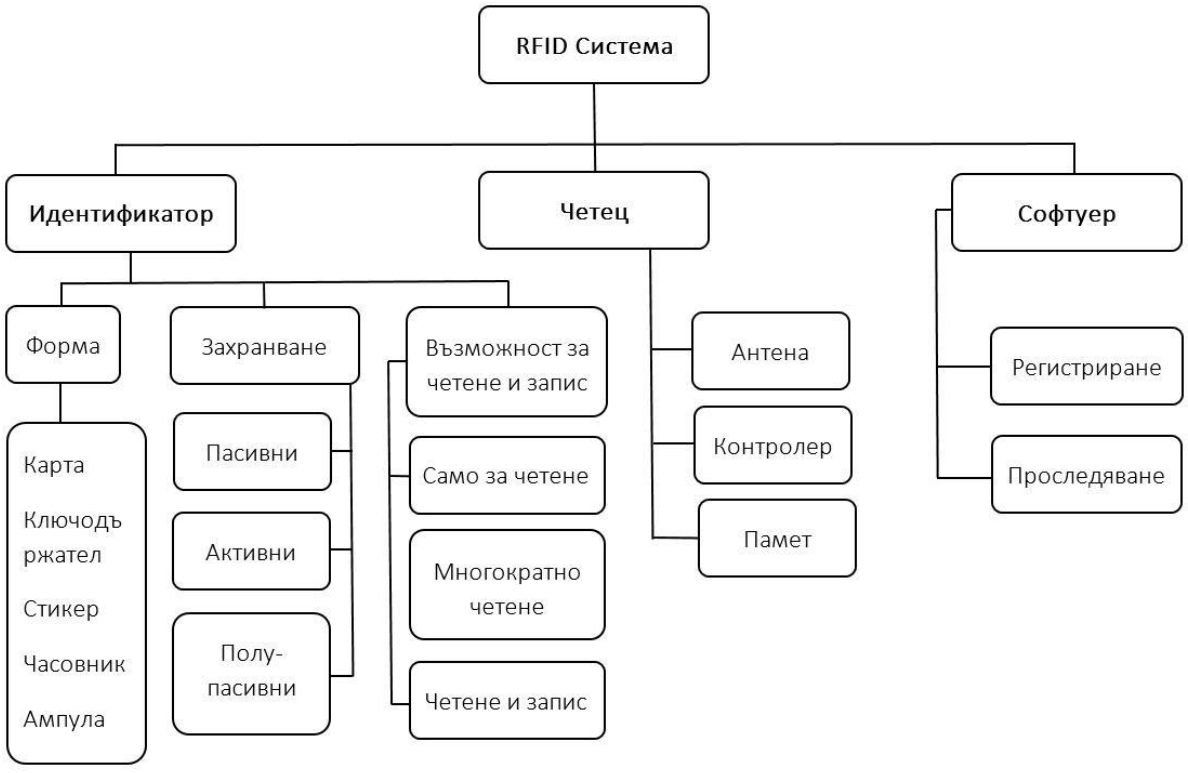
Софтуер

Софтуерът извършва обработка, съхраняване и визуализиране на информацията в RFID системите. Вариантите за софтуер са различни в зависимост от приложенията:

- регистриране на вход/изход в сграда, ограничаване на достъп и отчитане на време;
- регистриране на стоки и заприходяване в склад;
- проследяване на движение на идентификатор в производствена верига и др;

На база на натрупаната информация могат да бъдат подготвяни справки, да бъде изпращана информация към друга система, да се подават инструкции към контролера и т.н.

Комуникационната инфраструктура за свързване на сървъра с останалите компоненти на системата може да бъде осъществена безжично, чрез локална мрежа, сериен интерфейс и др.

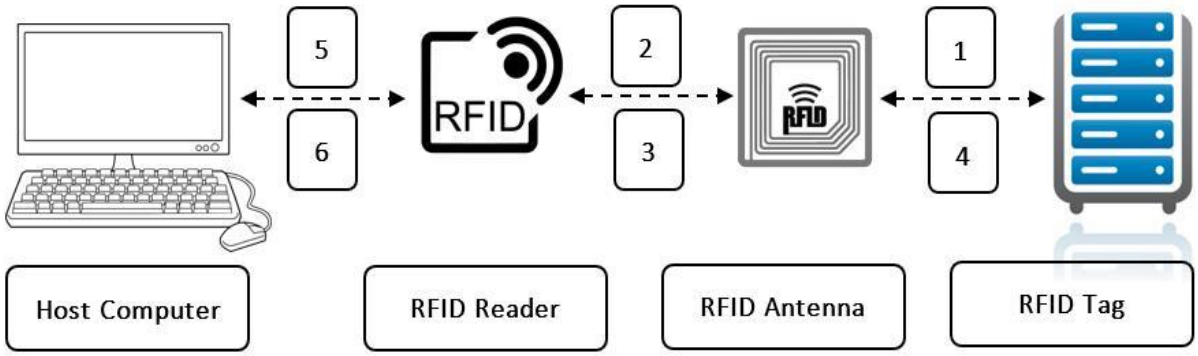


Фиг. 20 Компоненти на RFID системата

3.27.RFID технологията в библиотеките; Ползи от RFID технологията

Радио честотната идентификация (Radio Frequency Identification /RFID) е технология за безконтактно идентифициране на обекти . Тя позволява данните да бъдат бързо и автоматично прочетени. За разлика от баркода, RFID технологията позволява четене, записване и съхранение на данни върху използвания етикет, независимо от неговото разположение, заобикаляща среда, контакт или видимост. По този начин RFID отваря нови възможности в сферата на идентификацията, логистиката, управлението на материалните ресурси, производството и услугите.

Принципа на действие на RFID:



Фиг.20 Схема на принципа на действие на RFID

1 – RFID етикет влиза в радио честотно поле
2 – Сигналът на четеца активизира RFID
3 – Четецът изпраща модулиран сигнал
4 – Етикетът демодулира сигнала и връща данни към четеца
5 – Четецът изпраща данни към компютъра
6 – Компютърът изпраща нови данни чрез четеца към етикета

През 90-те години на миналият век, след като оценява значимостта и бъдещето на тази технология, 3M започва да работи по внедряването на RFID . Едно от най-динамичните направления на прилагане на RFID е в библиотечните системи. В резултат се появява цяла гама продукти, които имат за цел от една страна да облекчат труда на библиотечния служител, а от друга – да спестят време на читателите.

Приложението на RFID в библиотеките се свежда до използване на етикети с препрограмируеми микрочипове или т.нар. тагове (tags), които се залепват на корицата на книгата. Използваните от 3M тагове са с памет 1024b и 2048b и работят при честота 13,56 MHz (UHF). Стандартно върху тях се записва информацията от баркода (номера). На база този номер се извършва справка в библиотечната система.

Защо е така? Отговорът на този въпрос е в широко разпространената употреба на баркодовете в библиотечното дело. За усъвършенстване на една система от баркод към RFID е необходимо да се запази връзката между старата идентификация (баркод) и библиотечната система и новата идентификация (RFID). Това на практика означава при прочитане на баркод и RFID , залепени върху дадена книга да се получава еднозначна препратка към точно определена книга (инвентарен или каталожен номер) в библиотечната система. От тук следва, че най-добри резултати ще се получат когато номерата, прочетени от баркод четеца и RFID са идентични.

Компонентите на предлагана от 3M RFID система включват:

- Таг, който се състои от етикет, антена и идентификационен чип;
- Станция, която конвертира баркодовете към RFID ;
- Четец, който възпроизвежда информацията от RFID и позволява търсене, подреждане, връщане и инвентаризиране, като едновременно с това съхранява информация за библиотечния каталог;
- Работни станции, които обработват както баркодове, така и RFID и едновременно отписват и записват книги;
- Система за детекция, която предпазва от неоторизирано изнасяне от библиотеката;

3.30.Ползи от RFID технологията за библиотеките

RFID ускорява циркулациония процес в библиотеката. Информацията от RFID може да бъде прочетена значително по-бързо от тази от баркодовете, тъй като се избягва необходимостта от подравняване на тага с четеца. Едновременната проверка на няколко книги ускорява процеса на записване и отписване.

RFID позволява високо ниво на самообслужване в библиотеките. Потребителите могат да се възползват от изключително високата степен на автоматизация. Те могат лесно да заемат и връщат книги без намеса на библиотечен служител. RFID позволява автоматизирано сортиране като съкращава времето за подреждане на върнатите книги.

RFID защитава документите от неоторизирано изнасяне от библиотеката (въпреки, че не е със същата степен на ефективност както електромагнитната технология за защита). За постигане на максимален ефект 3M препоръчва EM защита в комбинация с RFID.

RFID позволява инвентаризация без да се налага изваждане на библиотечните документи от рафтовете, също така дава възможност за бързо търсене, намиране, връщане и преподреждане.

ЗАКЛЮЧЕНИЕ

Избраната тема за Магистърската теза е „Анализ на информационни системи за финансови институции и интернет сигурност“. Нейната основна цел е да изясни понятието Информационна система, видовете Информационни системи, основни термини свирзани с тях, етапите им на развитие, както и обвързаността им с Интернет сигурноста, Електронните разплащания и Електронното банкиране. Магистърската теза обхваща основните понятия за информационна сигурност и информационна система. Спира се по подробно на целите, изискванията и категориите информационна сигурност.

Магистърската теза представя системния подход към информационната сигурност и нейната структура. Също така са разгледани някои базови характеристики и обвързаността на информационната сигурност и бизнеса. В тезата са разгледани трите основни нива на информационна сигурност Базово, Средно и Високо ниво на информационна сигурност. Застъпено е по-подробно интернет банкирането, както и методите за сигурност свързани с него. Разгледана е системата и спецификата на безконтактните плащания, както и тяхната специфика, проблеми и сигурност.

Представени са някои заплахи и възможни защити при извършване на този вид он лайн дейности. Като основни модели за сигурност при интернет банкирането и други видове он лайн операции свързани с финансите са разгледани по подробно методите за уеб сигурност, криптиране и декриптиране на данни. Електронния подпис и Токен устройствата, който представляват отделен хардуер свързан със сигурноста на он лайн банкирането и други видове он лайн финансови операции.

От направения анализ на видовете информационни системи и интернетн банкиране може да се направи извода, че информационните системи са много широко застъпени в ежедневието във всички нива на обществения живот, а също така и бизнеса. В съвременните условия никоя фирма, предприятие или дейност не би могла да осъществява успешна дейност без използването на информационни системи и съпътстващите ги технологии.

Информационни системи се утвърждават като осъзната необходимост от фирмите във всички индустриални области, които активно и целенасочено се стремят към подобряване на ефективността и контрола над разходите с цел увеличаване на приходите.

Информационните системи осигуряват автоматизиране, интегриране и оптимизиране на бизнес процесите като по този начин позволяват канализиране на операциите, консолидиране на информацията и подпомагат вземането на управленски решения чрез различни възможности за анализ на информацията. По-конкретно, решенията се фокусират върху управление на процесите свързани с: финанси, счетоводство, верига за доставки, производство, планиране и логистика, човешки ресурси, склад, активи, проекти и отношения с клиентите.

Очакваните ползи от използването на бизнес управленски системи са свързни с възможността за вземане на адекватни управленски решения, оптимизиране и автоматизиране на основни бизнес процеси, по-добро пазарно позициониране, увеличаване ефективността на служителите, намаляване на оперативните разходи, подобряване на отношенията с клиентите и бизнес партньорите.

За постигането на добри резултати, т.е. подобряване на контролната среда, оптимизиране на контролните процедури и мерки, както от оперативна, така и от финансова гледна точка, организациите следва да дефинират стратегия за провеждането на одити на информационната среда, съобразена с общата бизнес стратегия. Провеждането на пълен детайлен одит на информационните системи за големи корпоративни структури от една страна е времеемко и съответно скъпоструващо начинание, а от друга страна, има и по-ниска ефективност.

Удачно е стратегията да включва бюджет за реализацията на планираните действия. Подобен бюджет се състои от пера за необходимото обучение на служителите, закупуване на автоматизирани средства за извършване на прегледи на информационната среда, разходи за външни ресурси, ако е необходимо и т.н. Не на последно място стратегията трябва да

включва определяне на структурната единица от организацията, която отговаря за контрола и прегледа на резултатите от одитите и за изпълнение на последващите действия

В заключение може да се посочи, че отговорността за установяване на ефективна вътрешна контролна среда, включително в областта на информационните технологии, е на ръководството на банковата институция. Контролната среда следва да поддържа бизнеса, като подпомага осигуряването му с достатъчна и качествена информация и да осигурява приемливо ниво на риск. Одитът на информационните системи е един основен компонент от функциите на вътрешния одит и неговото ефективно и компетентно изпълнение позволява да се реализират както оперативни, така и стратегически ползи за банката.

От анализа направен за безконтактните плащания могат да се направят следните изводи:

Безконтактната технология се базира на RFID технологията, работеща чрез микрочип и радио антена, което позволява предаване на информацията без физически контакт между картата и четящото устройство. Според извършени изследвания, докато плащането в брой отнема средно 34 секунди, при традиционните карти с магнитна лента са необходими 25 секунди, а при тези с RFID чип – едва 15 секунди. Също така, удобството при транзакциите изглежда оказва влияние и на желанието на потребителите на пазаруват. Доклад, публикуван преди няколко години сочи, че инсталирането на устройство за четене на безконтактни кредитни карти води до покачване от един процент на броя покупки в даден търговски пункт, а средната похарчена сума от клиентите скача с 15 на сто.

Други плюсове на новата технология са и че радиочестотните идентификатори могат да съдържат голямо количество информация, а четенето да се извършва без човешка намеса. Освен това, за разлика от магнитните ленти, чиповете са устойчиви на външни влияния като температурни промени, влага, химикали и др. Голямо предимство по отношение на сигурността при разплащане с безконтактна карта е, че не се налага картата да сепредоставя на трети лица в търговския обект при извършване на плащане. Няма основание за притеснение за това, че с безконтактна карта можете да се направи неволно плащане от разстояние. За да се осъществи успешна транзакция с безконтактна карта, е необходимо да картата да се намира до ПОС устройството на разстояние по–малко от 3 см. При успешна транзакция ПОС устройството издава светлинен и звуков сигнал, за информира, че е извършено плащане.

Като цяло сигурността на новата технология е добра, макар все пак да съществува минимален риск от кражба на данните. На теория това е възможнот посредство четец в мобилно устройство. Тъй като обаче за да бъде ефективен той е необходимо да се намира в непосредствена близост до самата карта, копиране на личните данни от нея би било изкючително трудно и неудобно и може лесно да бъде предодвратено ако се спазват елементарни мерки за сигурност, които всеки банков уеб сайт предоставя на своите ползватели. Технологията все още се популяризира и е напълно логично да се очакват подобрения както във ефективноста и, също и в сигурността. Все още дяловото участие на безконтактните плащания не е толкова високо, но тенденциите са към постоянното му увеличаване.

СПИСЪК НА ИЗПОЛЗВАНИТЕ ИЗТОЧНИЦИ

1. **Modern Information Systems**
Edited by Christos Kalloniatis, ISBN 978-953-51-0647-0, 174 pages, Publisher: InTech, Chapters published June 13, 2012 under CC BY 3.0 license
DOI: 10.5772/2886

2. **Management Information Systems: Managing the Digital Firm**
by Kenneth C. Laudon
2015 14th Revised edition
ISBN: 0133898164 / ISBN-13: 9780133898163

3. **Дальневосточного государственного университета путей сообщения**
http://www.dvgups.ru/

4. **Теория информационных процессов и систем**
Г.А. Доррер
Красноярск – 2008

5. **Финансови институции** - Википедия
https://bg.wikipedia.org/

6. **Търговски банки. Небанкови финансови институции**
http://www.lawsbg.com/lectures/65-commercial-law-lectures/223-turgovski-banki-sdelki.html

7. **УниКредит Булбанк**
Препоръки за сигурност при работа с интернет банкиране
http://www.unicreditbulbank.bg/en/index.htm

8. **Банковата система в България**
Джефри Милър, Стефан Петранов
Българска Народна Банка – Второ издание, София, 1996

9. **Окончателни насоки относно сигурността на плащанията в интернет**
European Banking Authority - EBA/GL/2014/12
19 декември 2014 г

10. **Българо-Американска Кредитна Банка АД**
Указания за работа с Интернет Банкирането

11. **Принцип работы технологии RFID и ее применение**
RTL-Service
http://rtlservice.com/company/rtlservice/

12. **RFID-технология**
http://www.rst-invent.ru/about/technology/