ГЛАВА 2
ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ БАНКІВСЬКОЇ БЕЗПЕКИ

2.1. Законодавча база банківської безпеки

В умовах інтеграції України у світове економічне співтовариство та в період посилення глобалізаційних процесів банківська галузь посідає провідне місце у розвитку національної економіки країни, а стабільне її функціонування є необхідною умовою для завоювання Україною міцних позицій на світовому ринку.

Відповідно до статті 4 Закону України «Про банки та банківську діяльність» банківська система України складається з Національного банку України та інших банків, а також філій іноземних банків, що створені і діють на території України відповідно до положення цього закону.

Рис. 2.1. Структура банківської системи України

Отже, банківська система України має дворівневу структуру рис. 2.1., 2.2.

Для забезпечення фінансової стабільності банківської системи НБУ здійснює регулювання та нагляд за діяльністю комерційних банків відповідно до положень Конституції України, Закону України «Про Національний банк України», Закону України «Про банки та банківську діяльність» та інших законодавчих та нормативно-правових актів Національного банку України.

Еволюцію розвитку банківської системи України можемо представити трьома періодами – становлення (перші п'ять етапів), другий – стабільності (шостий етап) та третій – кризовий (сьомий етап) (рис.2.3).

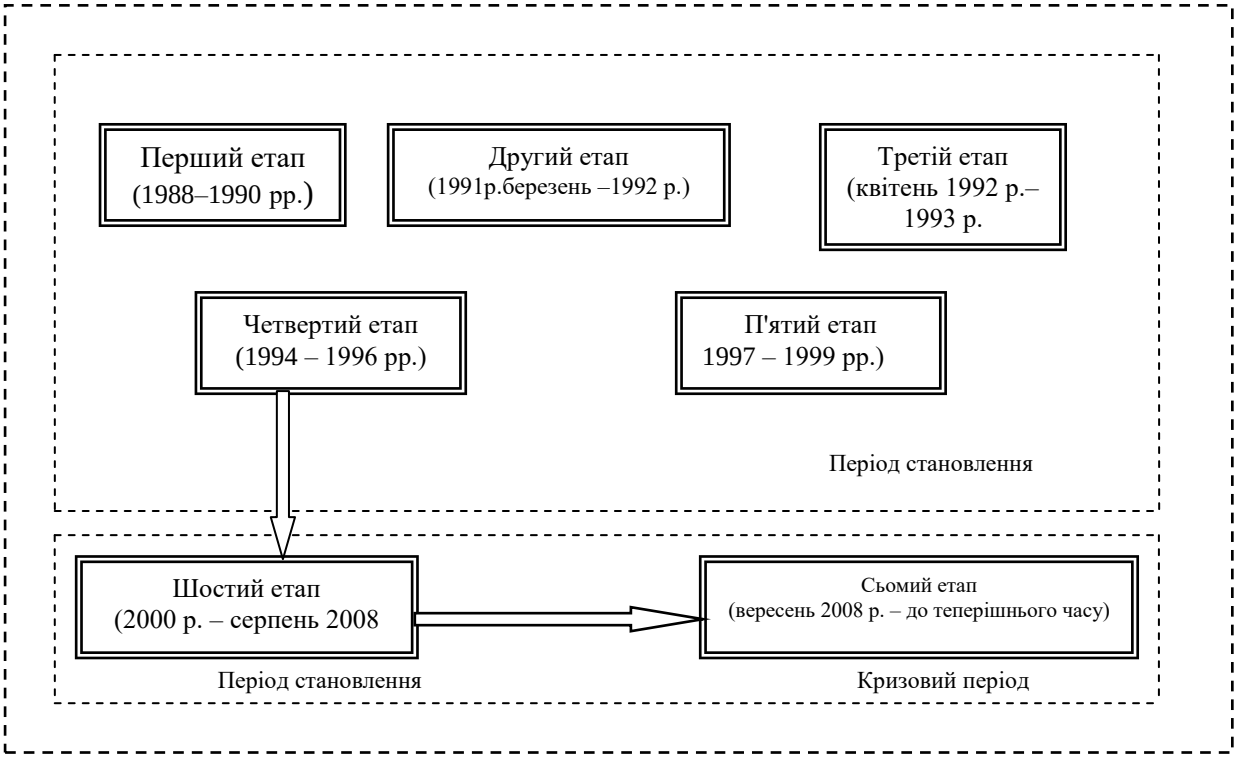

Рис. 2.2. Узагальнена схема етапів розвитку банківської системи України

Перший етап (1988 – 1990 рр.). Закладання загального фундаменту створення системи українських банків у складі банківської системи Радянського Союзу.

Другий етап (1991р. – березень 1992 р.). Законодавчою основою створення власної банківської системи стало прийняття Верховною Радою УРСР Закону «Про банки і банківську діяльність» в якому було закріплено створення дворівневої банківської системи.

У той же час розпочалися процеси перереєстрації та реорганізації банків. Із жовтня 1991 року НБУ почав перереєстрацію комерційних банків України,

що були зареєстровані ще Держбанком СРСР. У цей же період галузевий капітал, тобто частка капіталу, вкладеного у комерційні банки різними державними установами, поступово витіснялася ринковим капіталом спільних та малих підприємств, акціонерних товариств.

Третій етап (квітень 1992 р. – 1993 р.). Поява банків «нової хвилі» із залученням значного обсягу приватного капіталу та створення значної кількості дрібних «кишенькових» банків, які заробляли гроші лише з рахунок гіперінфляційних процесів в економіці. Недосконала нормативно-правова база та відсутність механізму впливу на комерційні банки з боку НБУ гальмували процес становлення банківської системи України.

Четвертий етап (1994 – 1996 рр.). На фоні скорочення грошової маси, призупинення швидкого зростання цін і тривалого спаду виробництва НБУ вибудував більш чітку систему регулювання діяльності комерційних банків. Неготовність великої кількості комерційних банків до центрального управління та жорстокого контролю з боку центрального банку призвело до їх банкрутства. У цей час з'явилися нові українські банки, відбувалася масова зміна складу акціонерів та власників комерційних банків та деяких їх філій шляхом продажу та перепродажу.

Ці події ускладнили роботу банківської системи України, так і всієї економіки в цілому, що підірвало довіру населення до банківської сфери.

Вихід країни з тривалої депресії супроводжувався успішним проведенням грошової реформи восени 1996 року, та введення в обіг національної грошової одиниці – гривні, що збалансувало економічні процеси в країні та підвищило інтерес зарубіжних інвесторів до української економіки. За даними НБУ, на кінець цього періоду було зареєстровано 14 іноземних банків та їх представництв на території України.

П'ятий етап (1997 – 1999 рр.). Удосконалення системи регулювання, поліпшення банківського нагляду на посилення контролю НБУ супроводжувалося світовою фінансово-економічною кризою, яка бере свій початок в Південно-Східній Азії 1997р.) і Росії (1998 р.), що ускладнило і без того нестійке економічне становище України. При цьому складалася неоднозначна ситуація – з одного боку, відбувалося закриття банківських установ у зв'язку з недостатністю ресурсів для їх функціонування, а з іншого – збільшилася частка залучення коштів на рахунки фізичних та юридичних осіб та обсягу незаконних кредитів.

Шостий етап (2000 р. – серпень 2008 р). Україна достойно пройшла етапи випробування і вийшла на новий рівень розвитку банківської системи на ринкових засадах в умовах розвитку глобалізаційних процесів. Складні періоди виживання сильніших банків завершилися, на зміну прийшов етап стабільності, що супроводжувався активною діяльністю НБУ та Уряду у розробці та прийняття нормативно-правових актів стосовно банківської діяльності та адаптації їх до стандартів Євросоюзу.

Інтенсивний розвиток банківської системи України був зумовлений стабільністю цін, заробітних плат, підвищенням ефективності виробництва, зменшенням рівня безробіття.

Сьомий етап (вересень 2008 р. – до теперішнього часу). Тільки в країні стабілізувалися економічні процеси, нахлинула друга хвиля невдач, яка зумовлена виникненням проблеми на іпотечному ринку США. В умовах динамічного розвитку глобалізаційних процесів на фінансовому ринку та інтеграції національних економік до світової, криза швидко перекинулася на інші країни світу, включаючи Україну. На кінець 2010 року частка іноземного капіталу у статутному капіталі банків складала приблизно 40,5%, що свідчить про залежність вітчизняних банків від закордонних і про неможливість ухилитися від процесів, які відбуваються на світовому фінансовому ринку. У цей час на тлі макроекономічних збурень зменшується ресурсний потенціал банківських установ зростає частка проблемних кредитів і, як наслідок отримані збитки. За 2008 – 2010 рр. Кредитна активність за коротко, середньостроковими – та за довгостроковими кредитами зменшилася але за довгостроковими значно більше. Основні зусилля регулюючих органів були направлені на зменшення частки проблемних кредитів у банківському секторі шляхом їх продажу та реструктуризації, оскільки частка простроченої заборгованості за кредитами зростає за аналізований період. Загальні зобов'язання банківських установ у 2009 році зменшилася в порівнянні з 2008 роком, що зумовлено економічною ситуацією в світі, коливанням валютного курсу гривні та заниження довіри до банківського сектора. Діяльність НБУ на цьому етапі була зосереджена на забезпеченні банківської стабільності та надійності, захисті прав вкладників та відновленні довіри суспільства.

Фінансово-кредитна система сукупність фінансових, інвестиційних і кредитних інститутів держави. Вона наведена на рис 2.3.

Рис.2.3. Структура фінансово-кредитної системи

Закони України передбачають наступне визначення: банк – юридична особа, яка на підставі банківської ліцензії має виключне право надавати банківські послуги, відомості про яку внесені до Державного реєстру банків.

У відповідності до передбачених функцій Банки — це фінансові установи, які здійснюють функції кредитування суб'єктів господарської діяльності

та громадян за рахунок залучення коштів підприємств, установ, організацій, населення та інших кредитних ресурсів, касового та розрахункового обслуговування господарства, виконання валютних та інших банківських операцій.

Закон України “Про Національний банк України” був опублікований у Відомостях Верховної Ради № 29, 1999 р., ст. 238. Згідно з положеннями Закону Національний банк України є центральним банком України, особливим центральним органом державним органом державного управління, юридичний статус, завдання, функції, повноваження й принципи організації якого визначаються Конституцією України, цим Законом та іншими законами України.

З точки зору захисту інформації у цьому Законі діє стаття 7 “Інші функції”. Згідно з цією статтею, Національний банк виконує такі функції:

п. 4: встановлює для банків правила проведення банківських операцій, бухгалтерського обліку і звітності, захисту інформації, коштів та майна;

п. 7: визначає напрями розвитку сучасних електронних банківських технологій, створює, координує та контролює створення електронних платіжних засобів, платіжних систем, автоматизації банківської діяльності та засобів захисту банківської інформації;

п. 18: реалізує державну політику з питань захисту державних секретів у системі Національного банку;

п. 22: здійснює методологічне забезпечення з питань зберігання, захисту, використання та розкриття інформації, що становить банківську таємницю

Метою цього Закону є правове забезпечення стабільного розвитку і діяльності банків в Україні й створення належного конкурентного середовища на фінансовому ринку, забезпечення захисту законних інтересів вкладників і клієнтів банків, створення сприятливих умов для розвитку економіки України та підтримки вітчизняного товаровиробника.

Цей Закон регулює відносини, що виникають під час заснування, реєстрації, діяльності, реорганізації та ліквідації банків.

Стаття 60 цього Закону «Банківська таємниця» вирішує питання пов’язані із забезпеченням інформаційної безпеки.

Інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним чи третіми особами при наданні послуг банку, є банківською таємницею.

Банківською таємницею, зокрема, є:

– відомості про банківські рахунки клієнтів, у тому числі кореспондентські рахунки банків у Національному банку України;

– операції, які були проведені на користь чи за дорученням клієнта, здійснені ним угоди;

– фінансово-економічний стан клієнтів;

– системи охорони банку та клієнтів;

– інформація про організаційно-правову структуру юридичної особи-клієнта, її керівників, напрями діяльності;

– відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація;

– інформація щодо звітності по окремому банку, за винятком тієї, що підлягає опублікуванню;

– коди, що використовуються банками для захисту інформації.

Інформація про банки чи клієнтів, отримана Національним банком України відповідно до міжнародного договору або за принципом взаємності від органу банківського нагляду іншої держави для використання з метою банківського нагляду або запобігання легалізації (відмиванню) доходів, одержаних злочинним шляхом, чи фінансуванню тероризму, становить банківську таємницю.

Положення цієї статті не поширюються на інформацію, яка підлягає опублікуванню. Перелік інформації, що підлягає обов'язковому опублікуванню, встановлюється Національним банком України та додатково самим банком на його розсуд.

Національний банк України видає нормативно-правові акти з питань зберігання, захисту, використання та розкриття інформації, що становить банківську таємницю, та надає роз'яснення щодо застосування таких актів.

Стаття 61 «Зобов’язання щодо збереження банківської таємниці» визначає зобов’язання, які повинні забезпечити банки щодо збереження банківської таємниці шляхом:

– обмеження кола осіб, що мають доступ до інформації, яка становить банківську таємницю;

– організації спеціального діловодства з документами, що містять банківську таємницю;

– застосування технічних засобів для запобігання несанкціонованому доступу до електронних та інших носіїв інформації;

– застосування застережень щодо збереження банківської таємниці та відповідальності за її розголошення у договорах і угодах між банком і клієнтом.

Службовці банку при вступі на посаду підписують зобов'язання щодо збереження банківської таємниці. Керівники та службовці банків зобов'язані не розголошувати та не використовувати з вигодою для себе чи для третіх осіб конфіденційну інформацію, яка стала відома їм при виконанні своїх службових обов'язків.

Банк має право надавати інформацію, яка містить банківську таємницю, приватним особам та організаціям для забезпечення виконання ними своїх функцій або надання послуг банку відповідно до укладених між такими

особами (організаціями) та банком договорів, у тому числі про відступлення права вимоги до клієнта, за умови, що передбачені договорами функції та/або послуги стосуються діяльності банку, яку він здійснює відповідно до статті 47 цього Закону. Приватні особи та організації, які при виконанні своїх функцій або наданні послуг банку безпосередньо чи опосередковано отримали конфіденційну інформацію, зобов'язані не розголошувати цю інформацію і не використовувати її на свою користь чи на користь третіх осіб.

У разі заподіяння банку чи його клієнту збитків шляхом витоку інформації про банки та їх клієнтів з органів, які уповноважені здійснювати банківський нагляд, збитки відшкодовуються винними органами.

Стаття 62 «Порядок розкриття банківської таємниці» визначає дуже важливі положення щодо розкриття таємниць, які має банк.

Інформація щодо юридичних та фізичних осіб, яка містить банківську таємницю, розкривається банками:

– на письмовий запит або з письмового дозволу власника інформації;

– за рішенням суду;

– органам прокуратури України, Служби безпеки України, Міністерства внутрішніх справ України, Антимонопольного комітету України – на їх письмову вимогу стосовно операцій за рахунками конкретної юридичної особи або фізичної особи – суб'єкта підприємницької діяльності за конкретний проміжок часу;

– органам Державної податкової служби України на їх письмову вимогу щодо наявності банківських рахунків;

– центральному органу виконавчої влади із спеціальним статусом з питань фінансового моніторингу на його запит щодо фінансових операцій, пов'язаних з фінансовими операціями, що стали об'єктом фінансового моніторингу (аналізу) згідно із законодавством щодо запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму, а також учасників зазначених операцій;

– органам державної виконавчої служби на їх письмову вимогу з питань виконання рішень судів та рішень, що підлягають примусовому виконанню відповідно до Закону України «Про виконавче провадження», стосовно стану рахунків конкретної юридичної особи або фізичної особи, фізичної особи – суб'єкта підприємницької діяльності.

Вимога відповідного державного органу на отримання інформації, яка містить банківську таємницю, повинна:

– бути викладена на бланку державного органу встановленої форми;

– бути надана за підписом керівника державного органу, скріпленого гербовою печаткою;

– містити передбачені цим Законом підстави для отримання цієї інформації;

– містити посилання на норми закону, відповідно до яких державний орган має право на отримання такої інформації.

Довідки по рахунках (вкладах) у разі смерті їх власників надаються банком особам, зазначеним власником рахунку (вкладу) в заповідальному розпорядженні банку, державним нотаріальним конторам або приватним нотаріусам, іноземним консульським установам по справах спадщини за рахунками (вкладами) померлих власників рахунків (вкладів).

Банку забороняється надавати інформацію про клієнтів іншого банку, навіть якщо їх імена, зазначені у документах, угодах та операціях клієнта.

Банк має право надавати інформацію, що становить банківську таємницю, іншим банкам та Національному банку України в обсягах, необхідних при наданні кредитів, банківських гарантій.

Банк має право розкривати інформацію, що містить банківську таємницю, особі (в тому числі яка уповноважена діяти від імені держави), на користь якої відчужуються активи та зобов'язання банку при виконанні заходів, передбачених програмою фінансового оздоровлення банку, або під час здійснення процедури ліквідації. Національний банк України (тимчасовий адміністратор) має право надавати Міністерству фінансів України інформацію, яка містить банківську таємницю щодо банків, участь у капіталізації яких бере держава.

Обмеження стосовно отримання інформації, що містить банківську таємницю, передбачені цією статтею, не поширюються на службовців Національного банку України або уповноважених ними осіб, які в межах повноважень, наданих Законом України «Про Національний банк України», здійснюють функції банківського нагляду або валютного контролю.

Національний банк України відповідно до міжнародного договору України або за принципом взаємності має право надавати інформацію, отриману при здійсненні нагляду за діяльністю банків, органу банківського нагляду іншої держави, а також отримувати від органу банківського нагляду

іншої держави таку інформацію. Надана (отримана) інформація може бути використана виключно з метою банківського нагляду або запобігання легалізації (відмиванню) доходів, одержаних злочинним шляхом, чи фінансуванню тероризму.

Положення частин другої та четвертої цієї статті не поширюються на випадки надання спеціально уповноваженому органу виконавчої влади з питань фінансового моніторингу інформації про фінансові операції у випадках, передбачених законом та органам державної податкової служби – інформації про відкриття (закриття) рахунків платників податків відповідно до статті 69 Податкового кодексу України.

Особи, винні в порушенні порядку розкриття та використання банківської таємниці, несуть відповідальність згідно із законами України.

Наступним законом у низці законів, що регламентують банківську діяльність є Закон України “Про платіжні системи та переказ грошей в Україні”. З позиції інформаційної безпеки біль детально слід розглянути Розділ 8. “Захист інформації при проведенні переказу”. До цього розділу входять статті 38, 39 і 40, які встановлюють вимоги щодо захисту інформації, відповідальність суб’єктів переказу за забезпечення захисту інформації та порядок надання інформаційних послуг.

Стаття 38. Вимоги щодо захисту інформації.

Стаття 38.1. Система захисту інформації повинна забезпечувати безперервний захист інформації щодо переказу коштів на усіх етапах її формування, обробки, передачі та зберігання.

Стаття 38.2. Електронні документи на переказ, розрахункові документи та документи за операціями із застосуванням спеціальних платіжних засобів, що містять банківську таємницю, під час їх передавання засобами телекомунікаційного зв'язку повинні бути зашифровані згідно з вимогами відповідної платіжної системи, а за їх відсутності - відповідно до законів України та нормативно-правових актів Національного банку України.

Стаття 38.3. Порядок захисту та використання засобів захисту інформації щодо переказу визначається законами України, нормативно-правовими актами Національного банку України та правилами платіжних систем.

Порядок захисту та використання засобів захисту інформації членами та учасниками міжнародних платіжних систем визначається правилами цих

систем, а за відсутності в таких правилах відповідних положень - законами України та нормативно-правовими актами Національного банку України.

Стаття 38.4. Захист інформації забезпечується суб'єктами переказу коштів шляхом обов'язкового впровадження та використання відповідної системи захисту, що складається з:

1) законодавчих актів України та інших нормативно-правових актів, а також внутрішніх нормативних актів суб'єктів переказу, що регулюють порядок доступу та роботи з відповідною інформацією, а також відповідальність за порушення цих правил;

2) заходів охорони приміщень, технічного обладнання відповідної платіжної системи та персоналу суб'єкта переказу;

3) технологічних та програмно-апаратних засобів криптографічного захисту інформації, що обробляється в платіжній системі.

Стаття 38.5. Система захисту інформації повинна забезпечувати:

1) цілісність інформації, що передається в платіжній системі, та компонентів платіжної системи;

2) конфіденційність інформації під час її обробки, передавання та зберігання в платіжній системі;

3) неможливість відмови ініціатора від факту передавання та отримувачем від факту прийняття документа на переказ, документа за операціями із застосуванням засобів ідентифікації, документа на відкликання;

4) забезпечення постійного та безперешкодного доступу до компонентів платіжної системи особам, які мають на це право або повноваження, визначені законодавством України, а також встановлені договором.

Стаття 38.6. Розробка заходів охорони, технологічних та програмно-апаратних засобів криптографічного захисту здійснюється платіжною організацією відповідної платіжної системи, її членами або іншою установою на їх замовлення.

Стаття 39. Відповідальність суб'єктів переказу за забезпечення захисту інформації

Стаття 39.1. Суб'єкти переказу зобов'язані виконувати встановлені законодавством України та правилами платіжних систем вимоги щодо захисту інформації, яка обробляється за допомогою цих платіжних систем. Правила платіжних систем мають передбачати відповідальність за порушення цих вимог з урахуванням вимог законодавства України.

Стаття 39.2. При проведенні переказу його суб'єкти мають здійснювати в межах своїх повноважень захист відповідної інформації від:

1) несанкціонованого доступу до інформації - доступу до інформації щодо переказу, що є банківською таємницею або є конфіденціальною інформацією, осіб, які не мають на це прав або повноважень, визначених законодавством України, а також якщо це не встановлено договором.

До банківської таємниці належить інформація, визначена Законом України «Про банки і банківську діяльність», а до конфіденціальної інформації - інформація, що визначається іншими законами.

Взаємодія між банками або іншими установами - учасниками платіжної системи та уповноваженими державними органами щодо надання на письмові запити цих органів інформації в межах, необхідних для виконання цими державними органами своїх функцій, здійснюється шляхом надання довідок в обсягах, визначених законодавством України, та з урахуванням вимог стосовно банківської таємниці та конфіденціальної інформації;

2) несанкціонованих змін інформації - внесення змін або часткового чи повного знищення інформації щодо переказу особами, які не мають на це права або повноважень, визначених законодавством України, а також встановлених договором;

3) несанкціонованих операцій з компонентами платіжних систем - використання або внесення змін до компонентів платіжної системи протягом її функціонування особами, які не мають на це права або повноважень, визначених законодавством України, а також встановлених договором.

Стаття 39.3. Суб'єкти переказу зобов'язані повідомляти платіжну організацію відповідної платіжної системи про випадки порушення вимог захисту інформації. У разі виявлення при цьому ознак, що можуть свідчити про вчинення злочину, суб'єкти переказу та інші учасники платіжних систем зобов'язані повідомити про такий випадок порушення вимог захисту інформації відповідні правоохоронні органи.

Стаття 39.4. Працівники суб'єктів переказу повинні виконувати вимоги щодо захисту інформації при здійсненні переказів, зберігати банківську таємницю та підтримувати конфіденційність інформації, що використовується в системі захисту цієї інформації.

Працівники суб'єктів переказу несуть відповідальність за неналежне використання та зберігання засобів захисту інформації, що використовуються при здійсненні переказів, відповідно до закону.

Стаття 39.5. Для належної ідентифікації суб'єктів помилкових та неналежних переказів та вжиття заходів щодо запобігання або припинення зазначених переказів члени платіжної системи повинні повідомляти інших членів системи про таких суб'єктів та перекази в обсягах, встановлених правилами відповідної платіжної системи або договорами між ними. Відповідно до договору та положень цього Закону зазначену діяльність може здійснювати спеціально визначена юридична особа, засновниками якої є члени платіжних систем. Члени платіжної системи та заснована ними юридична особа повинні забезпечити технологічний та програмно-апаратний захист персональних даних суб'єктів помилкових чи неналежних переказів згідно із цим Законом.

Стаття 40. Порядок надання інформаційних послуг

Стаття 40.1. Якщо член платіжної системи або його клієнт бере участь у розгляді спору судом, розрахунковий банк цієї платіжної системи чи клірингова установа зобов'язані надавати цьому члену платіжної системи або його клієнту, а також судам та органам досудового слідства послуги для визначення достовірності інформації, яка міститься в електронних документах, що обробляються платіжною системою, яку обслуговує цей розрахунковий банк, ця клірингова установа.

Суди та органи досудового слідства не можуть відмовити у прийнятті як доказу електронного документа та вимагати надання паперового документа.

Стаття 40.2. Порядок оплати членом платіжної системи або його клієнтом послуг, визначених пунктом 40.1 цієї статті, здійснюється за тарифами, встановленими розрахунковим банком.

Стаття 40-1. Порядок проведення моніторингу.

Еквайр та емітент повинні проводити моніторинг з метою ідентифікації помилкових та неналежних переказів, суб'єктів помилкових та неналежних переказів та вжиття заходів із запобігання або припинення зазначених переказів.

Моніторинг має проводитися постійно за параметрами, встановленими правилами відповідної платіжної системи.

Національний банк України може встановлювати загальні параметри моніторингу для всіх платіжних систем (груп платіжних систем).

За результатом моніторингу еквайр або емітент для належної ідентифікації суб'єкта переказу має право доручити торгівцю здійснити перевірку документів суб'єкту переказу. В інших випадках еквайр не має

права зобов'язувати торгівця, а торгівець не має права вимагати від держателя платіжної картки, суб'єкта переказу пред'явлення документів, що посвідчують особу, як засобу ідентифікації держателя, якщо це не передбачено правилами відповідної платіжної системи та /або умовами використання картки, встановленими емітентом.

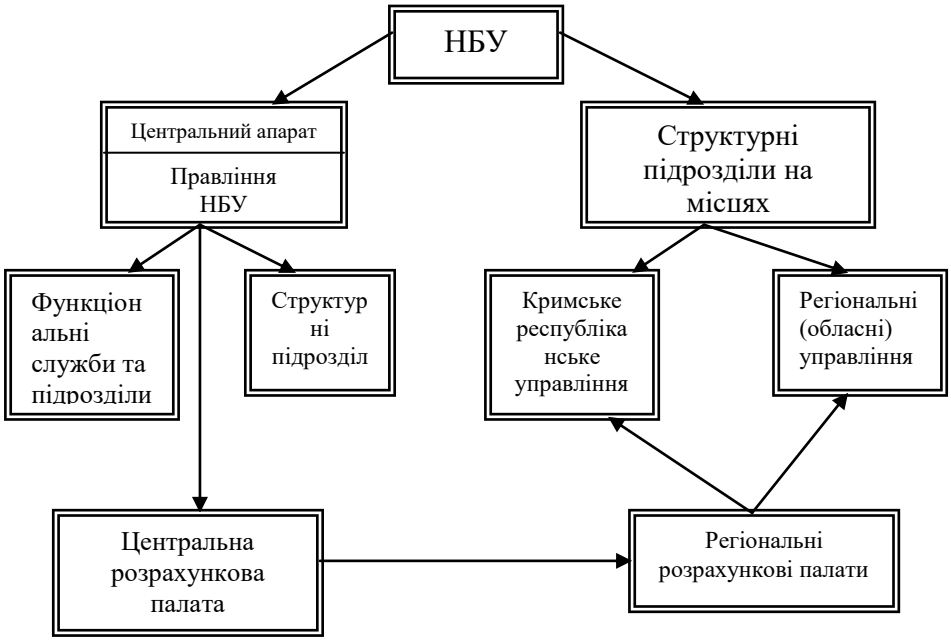

Рис. 2.3. Регіональна будова НБУ

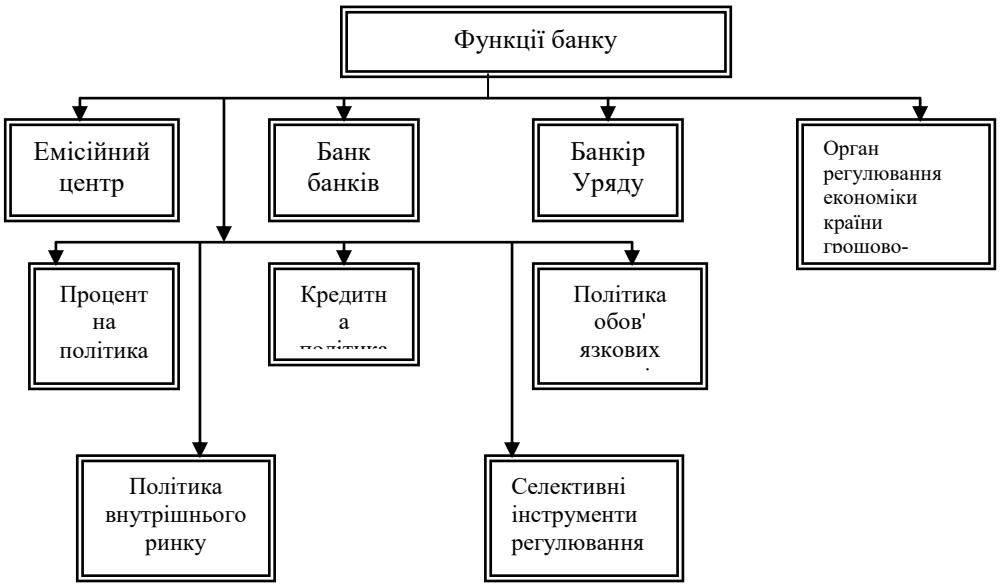

Рис.2.4. Функції банку

Порядок створення, державної реєстрації, ліцензування діяльності та реорганізації банків відображений в Законі України «Про банки та банківську діяльність», зокрема:

Стаття 14: «Учасники банків» (див. рис. 2.5.)

Стаття 15: «Найменування банку»;

Стаття 16: «Статут банку»;

Стаття 17: «Державна реєстрація юридичної особи, яка має намір здійснювати банківську діяльність»;

Стаття 18: «Підстави для відмови в погодженні статуту юридичної особи, яка має намір здійснювати банківську діяльність»

Національний банк України має право відмовити юридичній особі, яка має намір здійснювати банківську діяльність, у погодженні статуту, у разі якщо:

1) подано неповний пакет документів, необхідних для погодження статуту;

2) документи містять недостовірну інформацію;

3) документи не відповідають вимогам законів України чи нормативно-правових актів Національного банку України;

4) ділова репутація засновника, а для засновника - юридичної особи і членів її виконавчого органу та/або наглядової ради та всіх осіб, через яких здійснюватиметься опосередковане володіння істотною участю в банку, не відповідає вимогам, встановленим Національним банком України;

5) фінансовий стан засновника - юридичної особи та/або майновий стан засновника - фізичної особи не відповідають вимогам, встановленим Національним банком України;

6) засновник не має власних коштів для здійснення заявленого внеску до статутного капіталу;

7) структура власності самої юридичної особи, яка має намір здійснювати банківську діяльність, та/або засновника, що набуває істотної участі, не відповідає вимогам щодо її прозорості, встановленим Національним банком України;

8) не надано документи, що підтверджують наявність сплаченого статутного капіталу юридичної особи, яка має намір здійснювати банківську діяльність.

Національний банк України не має права відмовити юридичній особі, яка має намір здійснювати банківську діяльність, у погодженні статуту з інших підстав, крім зазначених у цій статті.

Стаття 19: «Банківська ліцензія»

Юридична особа, яка має намір здійснювати банківську діяльність, зобов'язана протягом року з дня державної реєстрації подати Національному банку України в порядку, визначеному цим Законом та нормативно-правовими актами Національного банку України, документи для отримання банківської ліцензії….

Стаття 19-1: «Підстави для відмови у видачі банківської ліцензії»

Національний банк України має право відмовити у видачі банківської ліцензії юридичній особі, яка має намір здійснювати банківську діяльність, у разі якщо:

1) подано неповний пакет документів, необхідних для видачі банківської ліцензії;

2) документи, подані для видачі банківської ліцензії, містять недостовірну інформацію;

3) документи, подані для видачі банківської ліцензії, не відповідають вимогам законів України та нормативно-правових актів Національного банку України;

4) юридична особа, яка має намір здійснювати банківську діяльність, звернулася із заявою про видачу банківської ліцензії після спливу річного терміну з дня її державної реєстрації;

5) професійна придатність та/або ділова репутація хоча б одного з керівників юридичної особи, яка має намір здійснювати банківську діяльність, та/або керівника її служби внутрішнього аудиту не відповідають вимогам, встановленим Національним банком України;

6) як мінімум три особи не призначені членами правління (ради директорів), у тому числі голова правління;

7) відсутні банківське обладнання, комп'ютерна техніка, програмне забезпечення, приміщення, що відповідають вимогам, встановленим Національним банком України.

Національний банк України має право відмовити у видачі банківської ліцензії юридичній особі, яка має намір здійснювати банківську діяльність, у разі невиконання її засновниками вимог частини сьомої статті 17 цього Закону.

Національний банк України зобов'язаний звернутися до суду з позовом про припинення юридичної особи у разі невиконання юридичною особою, яка має намір здійснювати банківську діяльність, протягом року з дня державної реєстрації вимог частини першої статті 19 цього Закону.

Стаття 20: «Підстави відкликання банківської ліцензії»

Національний банк України може відкликати банківську ліцензію виключно у таких випадках:

1) якщо було виявлено, що документи, надані для отримання ліцензії, містять недостовірну інформацію;

2) якщо банк не виконав жодної банківської операції протягом року з дня отримання банківської ліцензії;

3) у разі порушення цього Закону або нормативно-правових актів Національного банку України, що спричинило значну втрату активів і настання неплатоспроможності банку;

4) на підставі висновку тимчасового адміністратора про неможливість приведення банку у правову відповідність з вимогами цього Закону та нормативно-правових актів Національного банку України;

5) недоцільності виконання плану тимчасової адміністрації щодо реорганізації банку.

Стаття 23: «Порядок відкриття відокремлених підрозділів банку на території України»

Банк має право відкривати відокремлені підрозділи (філії, відділення, представництва тощо) на території України у разі його відповідності вимогам щодо відкриття відокремлених підрозділів, встановленим нормативно-правовими актами Національного банку України.

Банк зобов'язаний повідомити Національний банк України про відкриття відокремленого підрозділу.

Національний банк України включає відомості про відокремлені підрозділи банку до Державного реєстру банків на підставі письмового повідомлення банку.

Відокремлений підрозділ банку має право розпочати свою діяльність через 10 днів після повідомлення банком Національного банку України про відкриття такого відокремленого підрозділу.

Національний банк України має право прийняти рішення про припинення здійснення відокремленим підрозділом банку операцій на

користь або за дорученням клієнтів, якщо інформація про відкриття банком свого відокремленого підрозділу містить неправдиві відомості чи діяльність такого відокремленого підрозділу не відповідає вимогам цього Закону та нормативно-правовим актам Національного банку України.

Банк зобов'язаний повідомляти Національний банк України про зміни в документах та інформації, які надаються згідно з вимогами цієї статті, та надсилати Національному банку України копію рішення про внесення змін до положення про відокремлений підрозділ у двотижневий строк після його затвердження уповноваженим органом банку.

Банк зобов'язаний повідомити Національний банк України про прийняття уповноваженим органом банку рішення про закриття відокремленого підрозділу в семиденний строк після прийняття такого рішення та про фактичне припинення його діяльності – у триденний строк.

Таблиця 2.2.

Класифікаційні ознаки	**Види комерційних банків**
Порядок створення	Перепрофільовані, новостворені
Характер спеціалізації	Універсальні, спеціалізовані
Територія діяльності	Регіональні, республіканські, міжнародні
Розмір активів	Великі, середні, малі
Організаційно-правова форма	Публічні акціонерні товариства, кооперативні банки
Форма власності	Державні, приватні, зі стовідсотковою іноземною власністю, змішані
Форма організації	Державні, кооперативні, банківські об’єднання, банківська корпорація, банківська холдингова група, фінансова холдингова
Характер відносин	Банки-гаранти, банки-кореспонденти, уповноважені, регулятор
Ступінь контролю	Контролюючі, контрольовані (в т.ч. філії)
Фінансовий стан	Стабільні, проблемні, кризові, банкрути, в стадії ліквідації, з тимчасовою адміністрацією

Іноземні банки мають право *відкривати філії та представництва* на території України. [ст. 24 Закону України «Про банки та банківську діяльність»]. *Іноземний банк має право на відкриття філії* в Україні за таких умов:

– до держави, в якій зареєстровано іноземний банк, відсутні суттєві застереження з боку відповідних міжнародних органів щодо виконання нею міжнародних стандартів у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, та фінансуванню тероризму;

– банківський нагляд у державі, в якій зареєстровано іноземний банк, відповідає Основним принципам ефективного банківського нагляду Базельського комітету з питань банківського нагляду;

– між НБУ та органом банківського нагляду держави, в якій зареєстровано іноземний банк, укладено угоду про взаємодію у сфері банківського нагляду, гармонізації їх принципів та умов;

– мінімальний розмір приписного капіталу філії на момент її акредитації є не меншим 120 мільйонів гривень;

– наявність письмового зобов'язання іноземного банку про безумовне виконання ним зобов’язань, які виникли у зв'язку з діяльністю його філії на території України.

Акредитацію філій іноземних банків в Україні здійснює Національний банк України.

Акредитація філії іноземного банку здійснюється шляхом внесення відповідного запису до Державного реєстру банків та видачі банківської ліцензії.

Акредитація філії іноземного банку є підставою для здійснення нею банківської діяльності.

Діяльність філії іноземного банку повинна відповідати вимогам, встановленим Законом України «Про банки та банківську діяльність» та нормативно-правовим актам Національного банку України. Національний банк України здійснює регулювання діяльності та встановлює економічні нормативи для філій іноземних банків відповідно до вимог законодавства України.

Національний банк України має право відмовити в акредитації філії іноземного банку з таких підстав:

1) подані документи не відповідають вимогам цього Закону та нормативно-правових актів Національного банку України;

2) приміщення та обладнання філії не відповідають вимогам Національного банку України;

3) кандидатури керівника та головного бухгалтера філії не відповідають вимогам Закону України «Про банки та банківську діяльність» та нормативно-правових актів Національного банку України щодо професійної відповідності та ділової репутації;

4) в іноземного банку виявлено фінансові або правові проблеми, що вказують на можливість негативних наслідків для клієнтів чи потенційних клієнтів банку в результаті відкриття філії.

НБУ приймає рішення про акредитацію або відмову в акредитації філії іноземного банку протягом трьох місяців з моменту подання всіх необхідних документів. Відмова надається в письмовій формі із зазначенням відповідних підстав.

Філія іноземного банку здійснює свою діяльність відповідно до вимог, встановлених законами України для банків.

НБУ здійснює акредитацію представництв іноземних банк*ів* на території України в порядку та на умовах, визначених Законом України «Про банки та банківську діяльність» та нормативно-правовими актами НБУ.

Акредитація представництва іноземного банку здійснюється шляхом внесення відповідного запису до Державного реєстру банків.

Національний банк України може відмовити в акредитації представництва іноземного банку в разі порушення порядку акредитації, невідповідності поданих документів вимогам Закону України «Про банки та банківську діяльність» або нормативно-правових актів НБУ, недостовірності наданої інформації або перевищення повноважень щодо сфер діяльності представництва.

Рішення про акредитацію або відмову в акредитації представництва іноземного банку НБУ приймає протягом одного місяця з моменту подання всіх необхідних документів.

Відмова надається в письмовій формі із зазначенням відповідних підстав.

Національний банк України має право скасувати акредитацію представництва іноземного банку шляхом виключення відповідного запису з Державного реєстру банків у порядку, визначеному Національним банком України.

Офіційні документи, що подаються Національному банку України, повинні бути легалізовані в установленому порядку, якщо інше не передбачено міжнародними договорами, згода на обов'язковість яких надана

Верховною Радою України, та супроводжуватися нотаріально засвідченим перекладом українською мовою.

В 2003 році Верховною Радою України були прийняті два важливих Закони “Про електронний цифровий підпис” та “Про електронні документи та електронний документообіг”.

Закон України “Про електронний цифровий підпис” визначає правовий статус електронного цифрового підпису та регулює відносини, що виникають при використанні електронного цифрового підпису.

Цей Закон набрав чинності з 1 січня 2004 року. Введення в дію даного закону спричинило прийняття наступних документів:

1. Постанова КМУ №903 від 13.07.2004 «Про затвердження Порядку акредитації центру сертифікації ключів»

2. Постанова КМУ №1452 від 28.10.2004 «Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності»

3. Постанова КМУ №1454 від 28.10.2004 «Про затвердження Порядку обов'язкової передачі документованої інформації»

4. Постанова КМУ №551 від 21.05.2009 «Про заходи щодо запровадження системи електронної державної реєстрації юридичних осіб та фізичних осіб - підприємців»

За правовим статусом електронний цифровий підпис прирівнюється до власноручного підпису (печатки) в разі, коли:

– електронний цифровий підпис підтверджено з використанням посиленого сертифіката ключа за допомогою надійних засобів електронного цифрового підпису;

– під час перевірки використовувався посилений сертифікат ключа, чинний на момент накладання електронного цифрового підпису;

– особистий ключ підписувача відповідає відкритому ключу, зазначеному у сертифікаті.

Слід зазначити, що електронний цифровий підпис призначений для забезпечення діяльності юридичних і фізичних осіб із використанням електронних документів. Він використовується фізичними та юридичними особами для ідентифікації підписувача та підтвердження цілісності даних в електронній формі. Крім того, використання електронного цифрового підпису не змінює порядку підписання договорів та інших документів,

встановленого законом для вчинення правочинів у письмовій формі. Нотаріальні дії із засвідчення справжності електронного цифрового підпису на електронних документах вчиняються відповідно до порядку, встановленого законом.

Порядок застосування електронного цифрового підпису визначається Кабінетом Міністрів України, а порядок його застосування в банківській діяльності визначається Національним банком України згідно із Законом.

Сертифікат ключа містить обов’язкові дані, які наведені в статті 6 “Вимоги до сертифіката ключа.

Посилений сертифікат ключа, крім обов’язкових даних, які містяться в сертифікаті ключа, повинен мати ознаку посиленого сертифіката ключа.

Статті Закону 7 “Права та обов’язки підписувачів”, 8 “Центр сертифікації ключів”, 9 “Акредитований центр сертифікації ключів”, 10 “Засвідчувальний центр”, 11 “Центральний засвідчувальний орган” та 12 “Контрольний орган” роз’яснюють, які права має кожний із перерахованих суб’єктів взаємовідносин.

Відповідно до статті 15 “Відповідальність за порушення законодавства про електронний цифровий підпис” особи, що винні у порушенні законодавства з надання послуг електронного цифрового підпису, дії, що завдали матеріальної чи моральної шкоди юридичним або фізичним особам, несуть відповідальність згідно з Законом.

Закон України “Про електронні документи та електронний документообіг” встановлює основні організаційно-правові засади електронного документообігу та використання електронних документів.

Дія цього Закону поширюється на відносини, що виникають у процесі створення, відправлення, передавання, одержання, зберігання, оброблення, використання та знищення електронних документів.

Згідно із Законом, електронний документ – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа. Електронний документ може бути створено, передано, збережено, оброблено і перетворено у візуальну форму (відображення даних, які він містить, електронними засобами або на папері у формі, придатній для приймання його змісту людиною).

Відповідно до статті 6 Закону: Електронний підпис є обов'язковим реквізитом електронного документа, який використовується для ідентифікації автора та/або підписувача електронного документа іншими

суб'єктами електронного документообігу. Накладанням електронного підпису завершується створення електронного документа.

Стаття 7 «Оригінал електронного документу», визначає автентичність електронного документу а саме:

Оригіналом електронного документа вважається електронний примірник документа з обов'язковими реквізитами, у тому числі з електронним цифровим підписом автора.

У разі надсилання електронного документа кільком адресатам або його зберігання на кількох електронних носіях інформації кожний з електронних примірників вважається оригіналом електронного документа.

Якщо автором створюються ідентичні за документарною інформацією та реквізитами електронний документ та документ на папері, кожен з документів є оригіналом і має однакову юридичну силу.

Оригінал електронного документа повинен давати змогу довести його цілісність та справжність у порядку, визначеному законодавством; у визначених законодавством випадках може бути пред'явлений у візуальній формі відображення, в тому числі у паперовій копії.

Електронна копія електронного документа засвідчується у порядку, встановленому законом.

Копією документа на папері для електронного документа є візуальне подання електронного документа на папері, яке засвідчене в порядку, встановленому законодавством.

Юридична сила електронного документа не може бути заперечена виключно через те, що він має електронну форму. (стаття 8 «Правовий статус електронного документа та його копії»).

Нотаріальне посвідчення цивільно-правової угоди, укладеної шляхом створення електронного документа (електронних документів), здійснюється у порядку, встановленому законом.

Важливими статтями розділу ІІІ “Засади електронного документообігу” є статті 9 “Електронний документообіг”, 10 “Відправлення та передавання електронних документів”, 11 “Одержання електронних документів”, 12 “Перевірка цілісності електронного документа та 13 “Зберігання електронних документів та архіви електронних документів, які регламентують порядок проведення робіт з електронними документами».

Згідно з Законом, електронний документообіг (обіг електронних документів) – сукупність процесів складання, оброблення, передавання,

одержання, зберігання, використання електронних документів, які виконуються із застосуванням перевірки цілісності, справжності та у разі необхідності з підтвердженням факту таких документів.

Тому електронний документ вважається відправленим підписувачем, якщо він відправлений безпосередньо підписувачем або його електронною інформаційною системою, яка запрограмована на відправлення електронних документів в автоматичному режимі, а також посередником, уповноваженим підписувачем відправляти документи від його імені.

При цьому, електронний документ вважається одержаним адресатом з часу надходження авторові повідомлення в електронній формі від адресата про одержання цього електронного документа автора, якщо інше не передбачено законодавством або попередньою домовленістю між суб'єктами електронного документообігу.

У разі ненадходження до автора підтвердження про факт одержання електронного документа вважається, що електронний документ не одержано адресатом, і автор повинен вжити інших заходів до виконання своїх обов’язків перед адресатом.

Перевірка цілісності електронного документа проводиться шляхом перевірки електронного цифрового підпису.

При зберіганні електронних документів слід обов’язкове додержання таких умов:

– інформація, що міститься в електронних документах, повинна бути доступною для її подальшого використання;

– має бути забезпечена можливість відновлення електронного документа у тому форматі, в якому він був створений, відправлений або одержаний;

– у разі наявності повинна зберігатися інформація, яка дає змогу встановити походження та призначення електронного документа, а також дату і час його відправлення чи одержання.

Важливіший розділ цього Закону щодо охорони інформації є Розділ IV “Організація електронного документообігу”, який складається з 5-ти статей: стаття 14 “Організація електронного документообігу”, стаття 15 “Обіг електронних документів, що містять інформацію з обмеженим доступом”; стаття 16 “Права та обов’язки суб’єктів електронного документообігу”, стаття 17 “Вирішення спорів між суб’єктами електронного документообігу” та стаття 19 “Відповідальність за порушення законодавства про електронні документи та електронний документообіг”.

В цих статтях визначається, що використання електронних документів здійснюється відповідно до законодавства України або на підставі укладених договорів, що визначають взаємовідносини суб’єктів електронного документообігу.

Суб’єкти електронного документообігу, що здійснюють його на підставі укладених договорів, самостійно визначають режим доступу до електронних документів, які містять конфіденційну інформацію, та встановлюють для них систему (способи) захисту.

Засоби захисту інформації (ЗІ) та засоби цифрового підпису, які призначені для застосування в організації електронного документообігу, повинні бути сертифіковані або мати позитивний експертний висновок спеціально уповноваженого органу виконавчої влади у сфері криптографічного ЗІ.

Суб'єкти електронного документообігу користуються правами та мають обов'язки, які встановлено для них законодавством.

Якщо в процесі організації електронного документообігу виникає необхідність у визначенні додаткових прав та обов'язків суб'єктів електронного документообігу, що не визначені законодавством, такі права та обов'язки можуть встановлюватися цими суб'єктами на договірних засадах.

Особи, винні в порушенні законодавства про електронні документи та електронний документообіг, несуть відповідальність згідно з законами України.

В умовах постійно зростаючої комп'ютеризації й автоматизації передачі та збереження інформації особливого значення набуває захист даних, що існують в електронній формі.

У випадках, передбачених законом, доступ до інформації в системі може здійснюватися без дозволу її власника в порядку, встановленому законом.

Відносини між власником інформації та власником системи, власником системи та користувачем та між власниками систем розкриті в статтях 5–7. Окремо слід звернути увагу на те, що саме власник системи забезпечує захист інформації в системі в порядку та на умовах, визначених у договорі, який укладається ним із власником інформації, якщо інше не передбачено законом.

Умови обробки інформації в системі визначені в статті 8: Умови обробки інформації в системі визначаються власником системи відповідно до договору з власником інформації, якщо інше не передбачено законодавством.

Окремо відзначено, що інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством.

Для створення комплексної системи захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються в порядку, встановленому законодавством.

Стосовно захисту інформації в системі, у статті 9 відзначено:

Відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Власник системи, в якій обробляється інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним.

Повноваження державних органів у сфері захисту інформації в системах відзначені у статті 10.

Відповідно до абзацу 1 статті 10, вимоги до забезпечення захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, встановлюються Кабінетом Міністрів України. (на даний час такі вимоги визначені в Постанові КМУ від 29 березня 2006 року № 373 Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах).

Особливості захисту інформації в системах, які забезпечують банківську діяльність, встановлюються Національним банком України.

Особи, винні в порушенні законодавства про захист інформації в системах, несуть відповідальність згідно із законом (стаття 11 Закону).

Якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, визначено інші правила, ніж ті, що передбачені

цим Законом, застосовуються норми міжнародного договору. (стаття 12 Закону).

Кримінальний кодекс України ставить перед собою задачу – охорона суспільного ладу України, його політичної й економічної систем, власності, особистості, прав і свобод громадян і всього правопорядку від злочинних зазіхань.

Кримінальний кодекс України – це систематизована сукупність юридичних норм, установлених вищим органом законодавчої влади, що визначають, які суспільно небезпечні діяння є злочинними і які покарання варто застосовувати до осіб, що їх зробили.

Відповідно до чинного законодавства і Кримінального кодексу України, який прийнято та затверджено 5 квітня 2001 року № 2341-111, на злочинні дії з метою одержання інформації незаконним шляхом чи її зміни, знищення, розголошення, поширюються наступні статті Кримінального кодексу України.

Стаття 162. Порушення недоторканності житла.

Незаконне проникнення до житла чи до іншого володіння особи, незаконне проведення в них огляду чи обшуку, а так само незаконне виселення чи інші дії, що порушують недоторканність житла громадян, - карається штрафом від 50 до 100 неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до 2 років, або обмеженням волі на строк до 3 років.

Ті самі дії, вчинені службовою особою або із застосуванням насильства чи з погрозою його застосування, - карається позбавленням волі на строк від 2 до 5 років. Конституція України гарантує недоторканність житла. Не допускає проникнення в житло чи інше володіння особи, проведення в них огляду чи обшуку інакше як по мотивованому рішенню суду. У невідкладних випадках, зв'язаних із порятунком життя людей і майна чи з безпосереднім переслідуванням осіб, підозрюваних у здійсненні злочину, можливий інший, установлений законом, порядок проникнення в житло чи інше володіння особи, проведення в них огляду й обшуку (стаття 30 Конституції).

До дій, що порушують недоторканність житла громадян, відносяться: незаконний обшук, незаконне виселення чи інші дії. Під останніми варто розуміти незаконний огляд житла, незаконну виїмку речей, що у ньому знаходяться. Це може бути вселення в житло інших громадян без згоди тих, хто проживає в ньому.

Стаття 163. Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передається засобами зв'язку або через комп'ютер.

Ця стаття має дві частини:

Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передається засобами зв'язку або через комп'ютер, – карається штрафом від 50 до 100 неоподаткованих мінімумів доходів громадян або виправними роботами на строк до 2 років, або обмеженням волі до 3 років.

Ті самі дії, вчинені щодо державних чи громадських діячів або вчинені службовою особою, або з використанням спеціальних засобів, призначених для негласного зняття інформації, – карається позбавленням волі на строк від 3 до 7 років.

Таємниця листування, телефонних розмов і телеграфних повідомлень охороняється законом (ст. 31 Конституції України). Це означає, що ніхто не вправі без згоди самого громадянина знайомитися з його листуванням або розголошувати його зміст. Виключення можуть бути встановлені тільки судом у випадках, передбачених законом із метою запобігання злочину чи з'ясування істини під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо.

Стаття 330. Передача або збирання відомостей, що становлять конфіденційну інформацію, яка знаходиться у володінні держави.

Передача або збирання з метою передачі іноземним підприємствам, установам, організаціям або їх представникам економічних, науково – технічних або інших відомостей, що становлять конфіденційну інформацію, яка знаходиться у володінні держави, особою, якій ці відомості були довірені або стали відомі у зв'язку з виконанням службових обов'язків, за відсутності ознак державної зради або шпигунства, – караються обмеженням волі на строк до 3 років або позбавленням волі на строк від 2 до 5 років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до 3 років або без такого.

Ті самі дії, вчинені з корисливих мотивів, або такі, що спричинили тяжкі наслідки для інтересів держави, або вчинені повторно, або за попередньою змовою групою осіб, – карається позбавленням волі на строк від 4 до 8 років із позбавленням права обіймати певні посади або займатися певною діяльністю на строк до 3 років.

Предметом зазіхання в цьому випадку можуть бути тільки відомості, що складають службову таємницю в силу закону, постанови Кабінету Міністрів, розпорядження органів влади чи вказівки уповноваженого на те особи. Виток таких відомостей об’єктивно може нанести істотний майновий або інший збиток державної чи суспільної, чи іншої форми власності організаціям.

Передача таких відомостей припускає повідомлення їх зазначеній організації будь-яким способом. Вона можлива в усній чи письмовій формі (розповідь, лист, креслення, план, замальовка, аудіозапис, відео плівка і т. п.) і може бути здійснена особисто при зустрічі, під час розмови по телефону, по радіо, із використанням схованок, тварин, птахів, через посередників.

Стаття 359. Незаконні придбання, збут або використання спеціальних технічних засобів отримання інформації.

1. Незаконне придбання або збут спеціальних технічних засобів негласного отримання інформації, а також незаконне їх використання - караються штрафом від 200 до 1000 неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до 4 років, або позбавленням волі на той самий строк.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, - караються позбавленням волі на строк від 4 до 7 років.

3. Дії, передбачені частиною першою або другою цієї статті, вчинені організованою групою або якщо вони заподіяли істотну шкоду охоронюваним законом правам, свободам чи інтересам окремих громадян, державним чи громадським інтересам або інтересам окремих юридичних осіб, – караються позбавленням волі на строк від семи до десяти років.

Характерною ознакою ринкової економіки є конкуренція суб'єктів підприємницької діяльності на ринку товарів і послуг, успіх якої значною мірою залежить від здатності кожного з них зберігати в таємниці відомості про власну господарську й іншу діяльність і наявність таких відомостей про конкурентів.

Незаконне використання спеціальних технічних засобів негласного одержання інформації, варто розуміти одержання протиправним способом відомостей без наявності дозволу, тобто ліцензії на право застосування спеціальних технічних засобів.

Стаття 361. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

1. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації, - карається штрафом від 600 до 1000 неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від 2 до 5 років, або позбавленням волі на строк до 3 років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до 2 років або без такого та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, – караються позбавленням волі на строк від 3 до 6 років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи.

Примітка. Значною шкодою у статтях 361 - 363-1, якщо вона полягає у заподіянні матеріальних збитків, вважається така шкода, яка в 100 більше разів перевищує неоподатковуваний мінімум доходів громадян.

Стаття 361-1. Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут

1. Створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, – караються штрафом від 500 до 1000 неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до 2 років, або позбавленням волі на той самий строк, з конфіскацією програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, – караються позбавленням волі на

строк до 5 років з конфіскацією програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, які є власністю винної особи.

Стаття 361-2. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації.

1. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства, - караються штрафом від 500 до 1000 неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до 2 років з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані збут або розповсюдження інформації з обмеженим доступом, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, – караються позбавленням волі на строк від 2 до 5 років з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані збут або розповсюдження інформації з обмеженим доступом, які є власністю винної особи.

Стаття 362. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї

1. Несанкціоновані зміна, знищення або блокування інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, - караються штрафом від 600 до 1000 неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років з конфіскацією програмних або технічних засобів, за допомогою яких було вчинено несанкціоновані зміна, знищення або блокування інформації, які є власністю винної особи.

2. Несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації, - караються позбавленням волі на строк до 3 років з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк та з конфіскацією програмних чи технічних засобів, за допомогою яких було здійснено несанкціоновані перехоплення або копіювання інформації, які є власністю винної особи.

3. Дії, передбачені частиною першою або другою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, – караються позбавленням волі на строк від 3 до 6 років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до 3 років та з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані дії з інформацією, які є власністю винної особи.

Стаття 363. Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється

Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за їх експлуатацію, – караються штрафом від 500 до 1000 неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до 3 років з позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк.

Крім розглянутих статей Кримінального кодексу слід враховувати ще й деякі статті при вирішенні справ щодо економічної безпеки та комп’ютерної злочинності. Це, по-перше, стаття 200.

Стаття 200. Незаконні дії з документами на переказ, платіжними картами та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення.

1. Підробка документів на переказ, платіжних карток чи інших засобів доступу до банківських рахунків, а так само придбання, зберігання,

перевезення, пересилання з метою збуту підроблених документів на переказ чи платіжних карток або їх використання чи збут – карається штрафом від 3000 до 5000 неоподатковуваних мінімумів доходів громадян.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, – караються штрафом від 5000 до 10000 неоподатковуваних мінімумів доходів громадян.

Під документами на переказ слід розуміти документ в паперовому або електронному виді, що використовується банками чи їх клієнтами для передачі доручень або інформації на переказ грошових коштів між суб'єктами переказу грошових коштів (розрахункові документи, документи на переказ готівкових коштів, а також ті, що використовуються при проведенні міжбанківського переказу та платіжного повідомлення, інші).

У завершенні слід зазначити, що будь-яке підприємство зацікавлене в максимальному використанні свого права на захист інформації, але при цьому необхідно діяти тільки в рамках діючого законодавства і нормативних актів. Не слід забувати про те, що відповідальність за порушення законодавства про інформацію несуть особи, винні в здійсненні наступних дій:

– навмисне приховання інформації;

– примус до поширення чи перешкоджання поширенню, чи необґрунтоване відмовлення від поширення певної інформації;

– порушення порядку охорони інформації;

– необґрунтоване віднесення окремих видів інформації до категорії зведень з обмеженим доступом.

Варто мати на увазі, що порушення законодавства про інформацію спричиняє дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність.

Зокрема, якщо порушення порядку використання інформації, установленого законом, завдало істотної шкоди державним чи суспільним інтересам, охоронюваним законом правам і інтересам окремих фізичних чи юридичних осіб, то особа, визнана винною у даному діянні, може бути притягнута до кримінальної відповідальності по ст. 365 Кримінального кодексу України «Перевищення влади чи службових повноважень».

Таблиця 2.1

Види банківського кредитування

Класифікаційна ознака	Вид кредиту
Сфера використання	Внутрішній, Міжнародний, внутрішньобанківський, міжбанківський
Рівень банківської системи	Кредит Національного банку Кредит комерційного банку
Форма суспільного споживання	Фізичні особи, Юридичні особи
Характер витрат	Кредит в оборотні фонди, Кредит в основні фонди, споживчі, операції з цінними паперами
Термін використання	Короткостроковий (до одного року) Середньостроковий (1-3 роки) Довгостроковий (понад 3 роки)
Ступень майнового забезпечення	Забезпечений Незабезпечений, частково забезпечений

2.2. Нормативні акти банківської безпеки

Досить цікавими для підприємців можуть бути порядок і особливості захисту інформації, що представляє собою державну таємницю, а також правові взаємини й взаємозв'язок цієї інформації з комерційної таємниці (КТ) і конфіденційної інформації (КІ). Дані питання регулюються Законом України «Про державну таємницю», у відповідності, з яким державна таємниця (ДТ) – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою.

Слід зазначити, що Закон «Про державну таємницю» не торкається відносин, пов'язаних з охороною КТ чи КІ, якщо такі одночасно не є ДТ.

Віднесення відомостей до категорії ДТ здійснюється на підставі мотивованого рішення Державного експерта з питань таємниць з обов'язковим включенням їх у Перелік зведень, що являють собою ДТ.

Обов'язковим реквізитом будь-якого носія інформації, віднесеного до категорії ДТ, є гриф таємності, що повинний містити відомості про ступінь таємності («особливої важливості», «цілком таємно», «таємно»), терміну засекречування інформації та посадову особу, що встановила гриф. При цьому максимальні терміни, що можуть установлюватися для засекреченої

інформації, складають для грифа «особливо важлива» 30 років, «цілком таємно» – 10 років, «таємно» – 5 років.

Закон «Про державну таємницю» був прийнятий 21 січня 1994 року. Цей Закон регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, її засекречуванням і охороною з метою захисту життєво важливих інтересів України у сфері оборони, економіки, зовнішніх відносин, державної безпеки й охорони правопорядку.

Найбільш важливі і потрібні нам для *виконання діяльності з захисту інформації та технічного захисту інформації (ТЗІ) є наступні статті Закону*: стаття 6: «Здійснення права власності на секретну інформацію та її матеріальні носії»; стаття 8: «Інформація, що може бути віднесена до державної таємниці»; стаття 10: «Порядок віднесення інформації до державної таємниці»; стаття 12: «Звід відомостей, що становлять державну таємницю»; стаття 13: «Строк дії рішення про віднесення інформації до державної таємниці»; стаття 14: «Зміна ступеня секретності інформації та скасування рішення про віднесення її до державної таємниці»; стаття 15: «Засекречування та розсекречування матеріальних носіїв інформації»; стаття 18: «Основні організаційно-правові заходи щодо охорони державної таємниці»; стаття 19: «Єдині вимоги до матеріальних носіїв секретної інформації» і стаття 37: «Контроль за забезпеченням охорони державної таємниці».

Діючий Закон регламентує і визначає всі дії і заходи з охорони державної таємниці в Україні. Право держави на державну таємницю, на захист інформаційних ресурсів і технологій є загальноприйнятою нормою міжнародного права, і є незаперечним.

Окремо слід відзначити, що на підставі вищезазначеного закону Службою безпеки України був виданий наказ № 440 від 12.08.2005 року «Про затвердження Зводу відомостей, що становлять державну таємницю». В якому визначені наступні положення:

1. Відповідно до Закону України «Про державну таємницю» Звід відомостей, що становлять державну таємницю (далі – ЗВДТ), є єдиною формою реєстрації цих відомостей в Україні. З моменту опублікування ЗВДТ держава забезпечує захист і правову охорону відомостей, які зареєстровані в ньому.

ЗВДТ формується Службою безпеки України на підставі рішень державних експертів з питань таємниць про віднесення інформації до

державної таємниці та висновків державних експертів про скасування раніше прийнятих рішень, а у випадках, передбачених статтею 12 Закону України «Про державну таємницю» – на виконання рішень суду.

У разі включення до ЗВДТ інформації, яка не відповідає категоріям і вимогам, передбаченим статтею 8 Закону України «Про державну таємницю», або порушення встановленого порядку віднесення інформації до державної таємниці зацікавлені громадяни та юридичні особи мають право оскаржити відповідні рішення у судовому порядку.

2. Реєстрація відомостей у ЗВДТ є підставою для надання документу, виробу чи іншому матеріальному носію інформації, що містить ці відомості, грифа секретності, який відповідає ступеню секретності, установленому для них у ЗВДТ.»

Закон України «Про інформацію» закріплює право громадян України на інформацію і закладає правові основи інформаційної діяльності.

Закон введений у дію 2 жовтня 1992 року. Нова редакція закону була прийнята Верховною Радою 9 травня 2011 року на підставі Закону Україні «Про внесення змін до закону України «Про інформацію»« від 13 січня 2011 року.

З позицій організаційно-правового забезпечення нас цікавлять у першу чергу, наступні статті Закону:

Стаття 4: «Суб'єкти і об'єкти інформаційних відносин»;

стаття 6: п. 2 « Право на інформацію може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку, з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя»;

стаття 10: «Види інформації за змістом»;

стаття 11: «Інформація про фізичну особу»

«1. Інформація про фізичну особу (персональні дані) – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

2. Не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини. До конфіденційної інформації про фізичну особу

належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження.» (відносини, пов’язані із захистом персональних даних під час їх обробки регулює Закон України «Про захист персональних даних», який буде розглянуто далі);

Стаття 20: «Доступ до інформації».

«1. За порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом.

2. Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом».

Стаття 21: «Інформація з обмеженим доступом».

Одним із нормативних актів, що регулюють порядок охорони такої інформації, є Закон України “Про захист інформації в інформаційно-телекомунікаційних системах”, прийнятий у 2005 році, як нова редакція Закону “Про захист інформації в автоматизованих системах” (прийнятий 5 липня 1994 року).

Метою цього Закону є встановлення основ регулювання правових відносин у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно–телекомунікаційних системах.

У відповідності до статті 2 цього закону, об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

Стаття 3 «Суб'єкти відносин», визначає що, суб'єктами відносин, пов'язаних із захистом інформації в системах, є: власники інформації; власники системи; користувачі; спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації і підпорядковані йому регіональні органи.

В цієї ж статті відображенні умови договірні умови використання інформації, а саме: на підставі укладеного договору або за дорученням власник інформації може надати право розпоряджатися інформацією іншій фізичній або юридичній особі - розпоряднику інформації; на підставі укладеного договору або за дорученням власник системи може надати право розпоряджатися системою іншій фізичній або юридичній особі - розпоряднику системи.

Згідно зі *статтею 4* «Доступ до інформації в системі». Порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються власником інформації.

Порядок доступу до інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, перелік користувачів та їх повноваження стосовно цієї інформації визначаються законодавством.

Проблеми захисту інформації отримали подальший розвиток у Законах України “Про платіжні системи та переказ грошей в Україні”, “Про електронний цифровий підпис” та “Про електронні документи та електронний документообіг», «Про захист персональних даних», «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму« та ін.

У зв'язку з входженням України до Європейського союзу ключовими факторами, що зумовлюють адаптації вітчизняної банківської системи до міжнародних стандартів капіталом є посилення процесів глобалазації та фінансової інтеграції у банківському секторі, лібералізації руху капіталу, технологій та ризиків між країнами, зростання присутності іноземних банків у банківській системі країни, підвищення міжбанківської конкуренції, створення рівноправних регуляторних умов для функціонування вітчизняних та іноземних банків в Україні та за її межами.

Виходячи із аналізу вітчизняної банківської системи для перспективи адаптації банківської системи України до міжнародних стандартів управління капіталом ґрунтуються на комплексному використанні методів, що класифікуються за сферою і специфікою застосування на різних функціонально-ієрархічних рівнях управління вимог до забезпечення достатності власного банківського капіталу з метою забезпечення і індивідуальної стійкості банків в стабільних економічних умовах або під час економічної нестабільності. Це потребує кількісний обсяг та якісна структура регулятивного капіталу має покривати очікувані та неочікувані витрати від реалізації банківських ризиків – як індивідуальних, так і системних. У цьому контексті зазначено що індивідуальні банківські ризики корпоративних стратегій комерційних банків, які регулюються на рівні менеджменту кожного банку спеціальними методами ідентифікації, оцінювання та управління й не залежить від макроекономічних чинників. Натомість системні банківські ризики виникають внаслідок дії макроекономічних та

глобальних чинників (системних дисбалансів, економічних криз) і тому не можуть бути врегульовані на рівні корпоративного ризик–менеджменту банків. Це передбачає регламентацію регуляторних вимог до власного банківського капіталу як на рівні окремих банків, виходячи із специфіки іхньої діяльності та якості корпоративного управління так, і на рівні банківської системи кожної країни залежно від ступеня впливу системних ризиків та її функціонування. Зазначена концепція є регламентованою міжнародними стандартами управління капіталом банків та методологічного втілення в Базельських угодах про конвенцію капіталу.

В українській банківській практиці методичний підхід до оцінки достатності власного банківського капіталу ґрунтується на регламентаціях документа «Міжнародне наближення методів вимірювання і стандартів капіталу», який відрізняється від Угоди Базель I [35]. Однак інтеграція банківської системи України до Європейського співтовариства обумовлює потребу максимального наближення методичних підходів оцінки достатності капіталу до Базельських принципів. У зв'язку з цим необхідною є адаптація української регуляторної та корпоративної банківської практики до положень документів «Міжнародна конвергенція виміру капіталу і стандартів капіталу: нові підходи. Уточнена версія» (Базель II) [34] та «Глобальні регуляторні підходи для банків та банківських систем» (Базель III) [34] з урахуванням національних особливостей розвитку й функціонування банківської системи.

Зокрема за даними спільної місії МВФ та Світового банку від липня 2007 року в рамках Програми оцінки фінансового сектору України фахівцями визначено, що нормативи банківського нагляду, які діють в Україні, повністю відповідають Угоді про капітал Базель I (впроваджено 25 із 30 позицій Основних базельських принципів).

Основні напрямки впровадження в Україні Угоди Базель II задекларовано в Листі Національного банку України від 30.12.2004 року № 42–412/4010–13749, в якому пропонується впровадження трьох опор управління капіталом у зворотному порядку – від третьої до першої. Так, впровадження третьої компоненти Базель II «Ринкова дисципліна» планувалась здійснитись до 2007 року, другої компоненти «Процедура нагляду» до 2008 року, складової першої компоненти «Мінімальні вимоги до капіталу: кредитний ризик – стандартний підхід» – до 2010 року, «Мінімальні вимоги до капіталу: кредитний ризик – заснований на внутрішніх рейтингах» – до 2020 року, «Мінімальні вимоги до капіталу:

операційний ризик – підхід базового індикатора» – до 2010 року, «Мінімальні вимоги до капіталу: операційний ризик – стандартний підхід» – до 2015 року [34]. До сьогодні фактично було впроваджено ряд нормативно-правових актів, що стосуються формування систем ризик-менеджменту банків, впровадження нагляду на основі ризиків та покращання корпоративного управління у банківській сфері. Проте конкретних заходів щодо наближення вітчизняної банківської практики до положень першої компоненти Базеля ІІ наразі не було вжито. В Україні відсутнє відповідне правове поле щодо системного впровадження концепції оцінювання та управління системними та індивідуальними ризиками банків як на макро-, так і на мікроекономічному рівні. Окрім цього слід зазначити, що більшість із наведених у цих стандартах методик (вдосконалені ІКБ-підходи щодо оцінювання кредитного та операційного ризиків, методика розрахунку економічного капіталу) розраховані на країни з розвиненою економікою та ефективним функціонуванням фондового ринку. Україна, попри отримання статусу країни з ринковою економікою, наразі ще немає технічних можливостей для застосування сучасних моделей оцінювання ризиків через брак відповідних даних за багаторічний період щодо реалізації ризиків та нерозвиненістю елементів ринкової інфраструктури, зокрема рейтингових агентств. Так, рейтинг України було переглянуто у лютому 2009 року та встановлено на рівні «B-/C» і це задає межі рейтингів усіх компаній-резидентів. За такого рейтингу вимоги до позичальників українських банків повинні зважуватися за коефіцієнтом ризику 100 %, а для позичальників з рейтингом нижчим за «B-» зважування буде відбуватися за коефіцієнтом ризику 150%. Відтак у практиці адаптації вітчизняної банківської системи до положень Базеля ІІ це породжує ряд проблем щодо створення внутрішніх рейтингів позичальників; їх використання оцінок зовнішніх рейтингових агентств, зокрема міжнародних.

Як висновок, наближення банківської системи України до міжнародних стандартів управління капіталом відповідно до положень Угоди Базель ІІ потребує вирішення низки нормативно-правових, регуляторних, інституційних й методологічних питань, а також передбачає комплексне застосування методів адаптації як на державному рівні через органи законодавчої та виконавчої влади, національному регуляторному рівні шляхом посилення роботи Національного банку України, дорадчому регуляторному рівні внаслідок врахуванням пропозицій Асоціації

українських банків, так і на рівні корпоративного управління конкретних банків в напрямі належної організації процедур оцінки та управління ризиками та забезпечення відповідного рівня капіталізації банків. Підтверджує ці висновки й практика управління власним банківським капіталом в Україні за умов фінансово-економічної кризи.

Подолання цих перепон на рівні міжнародної банківської спільноти стимулювало б впровадження нових міжнародних стандартів управління капіталом – Базель ІІІ.

Виконання положень цієї угоди ставить перед банками завдання щодо «підвищення вимог до капіталу першого рівня, який має формуватися за рахунок звичайних акцій та нерозподіленого прибутку і перехід на концепцію антициклічного регулювання, врахування не тільки поточних, але й очікуваних втрат від ризиків; створення запасів капіталу понад регулятивного мінімуму»[36].

Вплив Угоди Базель ІІІ на діяльність українських банків щодо управління капіталом експерти прогнозують як невизначений»[34], оскільки рекомендації впроваджуються добровільно й передбачають поступовий перехід, а НБУ наразі не завершив впровадження Базель ІІ. Однак, опосередкований вплив відбуватиметься через механізм формування та використання банківського капіталу банками – представниками великих транснаціональних банків на території України, а також прийнятого Урядом політичного курсу щодо впровадження положень Базель ІІІ.

Отже, з огляду на необхідність впровадження у вітчизняну практику нових міжнародних підходів до банківського регулювання Національному банку України треба провести ґрунтовну роботу зі створення цілісної системи надання інформації різним економічним агентам щодо управління капіталом з урахуванням реальних банківських ризиків, удосконалення взаємодії регулятора з комерційними розробленнями інструментарію превентивних заходів впливу з огляду на ефективність управління власним капіталом.

Виходячи із вище зазначеного подальші перспективи адаптації банківської системи України до міжнародних стандартів управління капіталом ґрунтується на комплексному використанні спеціальних методів, що класифікуються за сферою і специфікою застосування на різних функціонально-ієрархічних рівнях управління таким чином як це представлено на рис. 2.6.

СОУ Н НБУ 65.1 СУІБ 1.0:2010. Стандарт організації України. Настанова. Методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги (*(ISO/IEC 27001:2005, MOD)*.

Цей стандарт є прийнятий зі змінами ***ISO/IEC*** 27001:2005. *Information technology – Security techniques – Information security management systems-Requirement* (Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги).

Цей стандарт має наступні розділи:

– вступ до ISO/IEC 27001:2005;
– сфера застосування;
– нормативні посилання;
– терміни та визначення понять;
– система управління інформаційною безпекою;

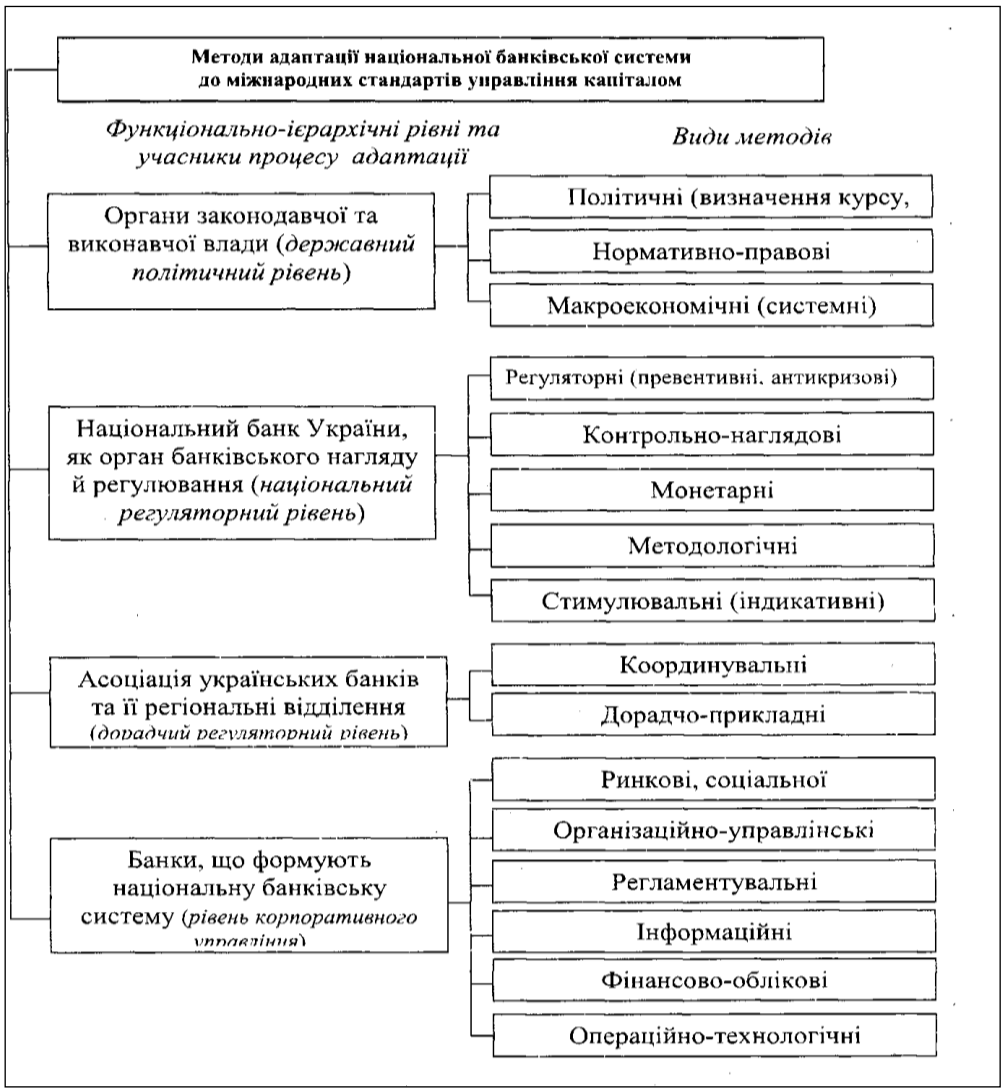

Рис.2.6. Методи адаптації національної банківської системи до міжнародних стандартів управління капіталом

– відповідальність керівництва;
– внутрішні аудити СУІБ;
– перегляд СУІБ з боку керівництва;
– вдосконалення СУІБ та додатки.

Цей стандарт створений для надання моделі розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування вдосконалення системи управління інформаційною безпекою (СУІБ). Прийняття СУІБ повинне бути стратегічним рішенням.

Цей стандарт розроблений для банків України і має використовуватися усіма банками України та їх підрозділами.

Стандарт приймає процесний підхід до розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення СУІБ банку.

Застосування системи процесів у межах банку разом з ідентифікацією цих процесів та їх взаємодіями, а також управління ними можна розглянути як процесний підхід.

Процесний підхід до управління інформаційною безпекою, запропонований цим стандартом, заохочує його користувачів робити наголос на важливості:

а) Розуміння вимог інформаційної безпеки організації і необхідності розроблення політики та цілей ІБ;

б) впровадження заходів безпеки та забезпечення їх функціонування для управління ризиками ІБ організації в контексті загальних бізнес-ризиків організації;

c) моніторингу та перегляді продуктивності та ефективності СУІБ;

d) постійному вдосконаленні, основаному на об'єктивному вимірюванні.

При розробці СУІБ банк повинен діяти таким чином:

а) Визначати сферу застосування та межі використання СУІБ виходячи з характеристик бізнесу, організації, його розташування, ресурсів СУІБ і технологій;

в) визначити політику СУІБ, виходячи з характеристик бізнесу, організації, його розташування, ресурсів СУІБ і технологій;

c) визначити підхід банку до оцінки ризику;

d) ідентифікувати ризики;

e) Проаналізувати та оцінити ризики;

f) ідентифікувати та оцінити альтернативні варіанти оброблення ризиків;

q) вибрати цілі заходів безпеки та заходи безпеки для оброблення ризиків;

h) отримати від керівництва затвердження запропонованих залишкових ризиків;

i) отримати санкцію керівництва на провадження та функціонування СУІБ;

j) підготувати Положення щодо застосування.

Щодо впровадження та функціонування СУІБ банк повинен діяти таким чином:

a) сформувати план обробки ризиків, який ідентифікує належні управлінські дії, ресурси, обов'язки та пріоритети щодо управління ризиками;

b) впровадити план оброблення ризиків для досягнення ідентифікаційних цілей заходів безпеки, який містить розгляд фінансових питань та розробку ролей і обов'язків;

c) для досягнення цілей заходів безпеки впровадити заходи безпеки;

d) визначити, як вимірювати ефективність вибраних заходів безпеки або груп заходів безпеки і встановити, як треба використовувати такі вимірювання для оцінки ефективності заходів безпеки;

e) впровадити програми з навчання та поінформованості;

f) управляти функціонуванням СУІБ;

q) управляти ресурсами СУІБ;

h) впровадити процедури та інші заходи безпеки для уможливлення термінового виявлення подій безпеки та реагування на інші заходи безпеки.

При моніторингу та перегляді СУІБ банк повинен діяти таким чином:

a) виконувати процедуру моніторингу та перегляду, а також інші заходи безпеки;

b) проводити регулярні перегляди ефективності СУІБ, враховуючи результати аудиторів безпеки, результати вимірювань ефективності, пропозиції і зворотній зв'язок з усіма зацікавленими сторонами;

c) вимірювати ефективність заходів безпеки, щоб підтвердити відповідність вимогам безпеки;

d) в заплановані терміни переглядати оцінки ризиків, а також переглядати залишкові ризики та ідентифіковані прийнятні рівні ризиків;

e) в заплановані терміни проводити внутрішні аудити СУІБ;

f) здійснювати на регулярній основі перегляд СУІБ з боку керівництва для забезпечення того, що сфера застосування залишається адекватною і вдосконалення в процесах СУІБ є ідентифікованими;

q) оновлювати плани впровадження заходів безпеки для врахування результатів діяльності з моніторингу та перегляду;

h) реєструвати дії та події, що можуть мати значний вплив на ефективність та продуктивність СУІБ.

У вимогах до документації повинна містити записи щодо управлінських рішень, забезпечуючи відстежуваність дій відповідно до управлінських рішень і політик, а також забезпечувати, що задокументовані результати відтворювані.

Важливо мати можливість продемонструвати зворотній зв'язок від вибраних заходів безпеки до результатів оцінки ризику і процесу оброблення ризику, а потім і до політики та цілей СУІБ.

Банк повинен в заплановані терміни проводити внутрішні аудити СУІБ для встановлення цілей заходів безпеки та процеси та процедури СУІБ:

a) відповідають вимогам цього стандарту та відповідному законодавству або нормативам;

b) відповідають вимогам ідентифікованої ІБ;

c) є ефективно впровадженими та підтримуваними, а також виконуються як очікувалося.

Керівництво повинне здійснювати перегляд СУІБ банку у заплановані терміни (не менше одного разу на рік) для забезпечення її постійної придатності, адекватності та ефективності. Цей перегляд повинен містити оцінку можливостей вдосконалення і потреби внесення змін у СУІБ, включаючи зміни у політиці ІБ і цілі ІБ. Результати такого перегляду повинні бути чітко задокументовані, а записи повинні підтримуватись.

Банк повинен постійно підвищувати ефективність СУІБ шляхом використання політики ІБ, цілей ІБ, результатів аудитів, подій, що підлягають моніторингу, коригуванню і запобіжних дій та перегляду з боку керівництва.

Банк повинен здійснювати дії для усунення причин невідповідностей вимогам СУІБ, щоб запобігти їх повторенню.

Банк повинен здійснювати дії для усунення причин потенційних невідповідностей вимогам СУІБ для запобігання їх появи. Здійснення запобіжних дій повинні відповідати величині впливу потенційних проблем.

Банк повинен ідентифікувати ризики, що змінилися. Та ідентифікувати вимоги до запобіжних дій, зосереджувати увагу на ризиках. Що істотно змінилися.

СОУ Н НБУ 65.1 СУІБ 2.0:2010. Стандарт організації України. Настанова. Методи захисту в банківській діяльності. Звіт правил для управління інформаційною безпекою *(ISO/IEC 27002:2005, MOD).*

Цей стандарт є прийнятий зі змінами міжнародний стандарт *ISO/IEC* 27002:2005 Information technology – Information technology – Code of practice for information security mantgmtnt (Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою).

Технічний комітет, відповідальний за цей стандарт – ТК 105 «Банківські та фінансові системи і технології».

Стандарт містить вимоги, які відповідають законодавству. До стандарту було внесено окремі зміни зумовлені правовими вимогами і конкретними потребами банківської сфери діяльності.

Інформація є ресурсом, який подібно іншим важливим бізнес-ресурсам, є суттєвим для бізнесу організації і тому потребує відповідного захисту. Це суттєво важливо у все більш взаємопов'язаному діловому середовищі. Внаслідок цієї зростаючої взаємопов'язаності інформація тепер наражається на зростаючу кількість і більшу різноманітність загроз та уразливостей.

Інформація може існувати у багатьох формах. Вона може бути надрукована або написана на папері, збережена в електронному вигляді, переслана поштою або з використанням електронних засобів, показана на плівці або сповіщена у бесіді. Незалежно від виду інформації або засобів, за допомогою яких вона поширюється або зберігається, інформація завжди повинна бути захищена відповідним чином.

Інформаційна безпека – це захист інформації від широкого діапазону загроз з метою забезпечення безперервності бізнесу, мінімізації бізнес-ризику і отримання максимальних рентабельності інвестицій і бізнес-можливостей.

Інформаційна безпека досягається впровадженням відповідного набору заходів безпеки, який охоплює політику, процеси, процедури, організаційні структури і програмні та апаратні функції. Ці заходи безпеки необхідно розробити, впровадити, здійснювати моніторинг, переглядати та. за необхідності, вдосконалювати для гарантування досягнення певного рівня

безпеки та бізнес-цілій організації. Це треба виконувати узгоджено з іншими процесами управління бізнесом.

СОУ Н НБУ 65.1 СУІБ 2.0:2010

0.1. Що таке інформаційна безпека?

Інформація є ресурсом, який подібно іншим важливим бізнес-ресурсам, є суттєвим для бізнесу організації і тому потребує відповідного захисту. Це суттєво важливо у все більш взаємопов'язаному діловому середовищі. Внаслідок цієї зростаючої взаємопов'язаності інформація тепер наражається на зростаючу кількість і більшу різноманітність загроз та уразливостей.

Інформація може існувати у багатьох формах. Вона може бути надрукована або написана на папері, збережена в електронному вигляді, переслана поштою або з використанням електронних засобів, показана на плівці або сповіщена у бесіді. Незалежно від виду інформації або засобів, за допомогою яких вона поширюється або зберігається, інформація завжди повинна бути захищена відповідним чином.

Інформаційна безпека – це захист інформації від широкого діапазону загроз з метою забезпечення безперервності бізнесу, мінімізації бізнес-ризику і отримання максимальних рентабельності інвестицій і бізнес-можливостей.

Інформаційна безпека досягається впровадженням відповідного набору заходів безпеки, який охоплює політику, процеси, процедури, організаційні структури і програмні та апаратні функції. Ці заходи безпеки необхідно розробити, впровадити, здійснювати моніторинг, переглядати та. за необхідності, вдосконалювати для гарантування досягнення певного рівня безпеки та бізнес-цілій організації. Це треба виконувати узгоджено з іншими процесами управління бізнесом.

0.2 Навіщо потрібна інформаційна безпека?

Інформація та допоміжні процеси, системи і мережі є важливими бізнес - ресурсами системи управління інформаційною безпекою (СУІБ). Визначенню досягнення, підтримка та вдосконалення інформаційної безпеки може бути суттєвим для підтримки конкурентоспроможності, готівкового обігу, рентабельності, комерційної репутації та відповідності законодавству .

Організації та їхні інформаційні системи й мережі натрапляють на загрози безпеці від широкого кола джерел, включаючи комп'ютерне шахрайство – шпіонаж, саботаж, вандалізм, пожежу або повінь. Причини

порушень типу зловмисних кодів, комп'ютерного хакерства і атак типу відмови в обслуговуванні стали більш поширеними і значно досконалішими.

Інформаційна безпека є важливою як для державного і приватного секторі бізнесу, так і для захисту критичних інфраструктур. В обох секторах інформаційна безпека буде працювати як фактор сприяння, наприклад, в електронному урядуванні або електронному бізнесі, або для уникнення чи зменшення відповідних ризиків. Взаємозв'язок загальнодоступних і приватних мереж та спільне використання інформаційних ресурс в збільшують труднощі в досягненні контролю доступу. Тенденція до розподіленого оброблення даних може також послабити ефективність централізованого, фахового контролю. Багато інформаційних систем не проектувалися як безпечні. Безпека, яка може бути досягнута за допомогою технічних засобів, є обмеженою і мас підтримуватись відповідним управлінням та процедурами. Визначення, які заходи безпеки треба застосовувати на місці, вимагає ретельного планування та уваги до дрібниць. Управління інформаційною безпекою вимагає щонайменше участі СОУ Н НБУ 65.1 СУІБ 2.0:2010 всього персоналу організації. Воно може також вимагати співучасті від акціонерів, постачальнице, третіх сторін, користувачів або інших зовнішніх сторін.

Рекомендації фахівців із сторонніх організацій також можуть стати в нагоді.

0.3 Як розробити вимоги безпеки

Організація повинна ідентифікувати свої вимоги безпеки. С три основні джерела формування вимог безпеки.

1. Одним джерелом є результат оцінки ризиків для організації, який враховує загальну бізнес-стратегію та цілі. Під час оцінювання ризику ідентифікують загрози ресурсам СУІБ і оцінюють вразливість та ймовірність подій і визначають величину потенційного впливу.
2. Іншим джерелом є правові вимоги, ті. що існують на підставі законодавства, нормативні та контрактні вимоги, яким організація, її партнери, підрядники та постачальники послуг повинні відповідати, а також їх соціально-культурне середовище.
3. Ще одним джерелом є власний набір принципів, цілей та бізнес-вимог щодо оброблення інформації, який організація розробила для підтримки свого функціонування.

0.4 Оцінка ризиків безпеки

Вимоги безпеки ідентифікуються систематичною оцінкою ризиків безпеки. Витрати на заходи безпеки повинні бути збалансовані з бізнес-втратами, які можуть бути наслідком порушень безпеки.

Результати оцінки ризику допомагатимуть спрямувати і визначити відповідні управлінські дії та пріоритети управління ризиками інформаційної безпеки і впровадження заходів безпеки, вибраних для захисту від цих ризиків.

Оцінка ризиків повинна періодично повторюватися для врахування будь-яких змін, які можуть вплинути на результати оцінки ризику.

0.5 Вибір заходів безпеки

Після ідентифікації вимог безпеки та ризиків і прийняття рішення щодо оброблення ризиків, необхідно вибрати та впровадити відповідні заходи безпеки для забезпечення зниження ризиків до прийнятного рівня. Заходи безпеки можна вибирати з цього стандарту або інших наборів заходів, або, якщо необхідно, можна спроектувати нові заходи безпеки для задоволення певних потреб. Вибір заходів безпеки залежить від управлінських рішень, основаних на критеріях прийняття ризику, варіантах обробки ризику та загальному підході до управління ризиком, застосовному в організації, він повинен також відповідати усьому чинному національному й міжнародному законодавству та нормативним документам.

Деякі з заходів безпеки в цьому стандарті можуть розглядатися як настановні принципи щодо управління інформаційною безпекою, які можуть бути застосовані для більшості організацій. Вони пояснюються більш детально нижче під заголовком «Відправна точка інформаційної безпеки.

0.6 Відправна точка інформаційної безпеки

Низку заходів безпеки можна розглядати як хорошу відправну точку для впровадження інформаційної безпеки. Вони або базуються на основних законодавчих вимогах, або розглядаються як звичайна практика інформаційної безпеки.

Заходи безпеки, які вважаються важливими для організації з законодавчої точки зору, містять, залежно від застосовного законодавства:

a) захист даних та конфіденційність персональних даних:

b) захист організаційних записів;

c) права інтелектуальної власності.

Треба зазначити, що хоча всі заходи безпеки в цьому стандарті є важливими і повинні бути розглянутими, важливість кожного заходу повинна визначатися з позицій певного ризику, з яким стикається організація. Отже, хоча вищевикладений підхід розглядається як хороша відправна точка, він не замінює вибору заходів безпеки, основаного на оцінці ризику.

0.7 Критичні фактори успіху

Досвід показує, що нижченаведені фактори часто є критичними для успішного впровадження інформаційної безпеки в організації:

a) політика інформаційної безпеки, цілі та діяльність, які відображують цілі бізнесу;

b) методи та основні правила впровадження, підтримання, моніторингу та вдосконалення інформаційної безпеки, сумісні з культурою організації;

c) очевидна підтримка та зобов'язання керівництва усіх рівнів;

d) добре розуміння вимог інформаційної безпеки, оцінки ризику та управління ризиком;

e) ефективне доведення та роз'яснення інформаційної безпеки всім СОУ Н НБУ 65.1 СУІБ 2.0:2010 керівникам, працівникам та іншим сторонам для досягнення поінформованості;

f) розповсюдження настанов щодо політики інформаційної безпеки та стандартів всім керівникам, працівникам та іншим сторонам;

g) забезпечення фінансування діяльності з управління інформаційною безпекою;

h) забезпечення відповідних поінформованості, навчання та освіти;

i) розроблення ефективного процесу управління інцидентами інформаційної безпеки:

j) впровадження системи вимірювань, яка використовується для оцінювання продуктивності управління інформаційною безпекою і пропозицій зворотного зв'язку для вдосконалення.

0.8 Розвиток ваших власних настанов

Цей звід правил може розцінюватись як відправна точка для розвитку певних конкретних настанов організації. Не всі заходи безпеки та настанови з цього зводу правил можуть бути застосовні. Крім того, можуть бути потрібні додаткові заходи безпеки та настанови, які не включені до цього стандарту. Під час розроблення документів, які містять додаткові настанови чи заходи безпеки, може бути корисним наводити в тих місцях, де це необхідно,

перехресні посилання на розділи цього стандарту для полегшення перевірки відповідності аудиторами та бізнес-партнерами.

Треба зазначити, що вимірювання інформаційної безпеки виходять за межі цього стандарту.

Сфера застосування

Цей стандарт встановлює настанови та загальні принципи щодо започаткування, впровадження, підтримки та вдосконалення управління інформаційною безпекою в організаціях. Цілі, окреслені в цьому стандарті, надають основні настанови щодо загальноприйнятих цілей управління інформаційною безпекою.

Цей стандарт розроблений для банків України і має використовуватися усіма банками України та їх підрозділами. Цілі заходів безпеки та заходи безпеки цього стандарту призначені для впровадження з метою задоволення вимог, ідентифікованих оцінкою ризику. Цей стандарт є практичною настановою для розвитку стандартів безпеки в організаціях та практики ефективного управління безпекою, і для допомоги в побудові конфіденційності в діяльності організації.