А.О.Корченко
Л.М.Скачек
В.О.Хорошко

БАНКІВСЬКА БЕЗПЕКА

Київ 2014

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний авіаційний університет

А.О.Корченко, Л.М.Скачек, В.О.Хорошко

БАНКІВСЬКА БЕЗПЕКА

Підручник

За загальною редакцією доктора технічних наук, професора

Хорошка В.О.

Київ – 2014

УДК 336.71:004.056:34

ББК 65.262.1

Б 45

Затверджено на засіданні Науково-методично-редакційної ради Інституту комп'ютерних технологій НАУ (протокол № 3 від 12.11.2014 р.)

Рецензенти: доктор технічних наук, професор Засядько А.А.

доктор юридичних наук, професор Шакун В.І.

доктор економічних наук, професор Живко З.Б.

Б 45

Банківська безпека: Підручник / КорченкоА.О., Скачек Л.М, Хорошко В.О. /За заг. ред. докт. техн. наук, проф. О.В.Хорошка. – К.: ПВП «Задруга», 2014 – с.185.

ISBN 978-966-2970-82-1

У підручнику надаються методи та засоби здобуття інформації щодо банківської діяльності, а також організації комерційної та конфіденційної таємниць банків. Розглядаються правові основи банківської діяльності та правове забезпечення захисту банківської інформації, ризики та їх оцінка у банківській діяльності, злочини та забезпечення безпеки.

Видання має стати у пригоді працівникам підрозділів безпеки банків, а також працівникам банків, студентам та аспірантам вищих навчальних закладів.

УДК 336.71:004.056:34

ББК 65.262.1

ISBN 978-966-2970-90-6

ЗМІСТ

СКОРОЧЕННЯ

АС – автоматизована система

АСОД – автоматизована система обробки даних

БІС – банківська інформаційна система

БР – банківський рахунок

ДПА – Державна податкова адміністрація

ДСТСЗІ – Департамент спеціальних телекомунікацій та захисту інформації

ДТ – державна таємниця

ЗВДТ – звід відомостей, що становлять державну таємницю

ЕОМСМ – електронно-обчислювальні машини, системи мережі

ІЗТОО – інженерний захист і технічна охорона об'єкта

ІС – інформаційна система

ІБ – інформаційна безпека

КВІ – канал витоку інформації

КІ – конфіденційна інформація

КТ – комерційна таємниця

НБУ – Національний банк України

СБ – служба безпеки

СУІБ – система управління ІБ

ТЗІ – технічний захист інформації

ОЗГ– організована злочинна група

ПД – персональні дані

ОД – об'єкт захисту

ЗІ – захист інформації

МІЗІП – матриця інформаційної зв’язаності інформаційного процесу

ВМІП – варіаційна матриця інформаційного процесу

КР – конкурентна розвідка

ІБ – інформаційна безпека

ПІБ – прізвище ім'я по-батькові

ДПА – державна податкова адміністрація

ПЕОМ – персональна електронно-обчислювальна машина

ВСТУП

Важливе значення в забезпеченні безпеки України, а особливо економічної, має захист її ринкових основ і, перш за все, захист економічної конкуренції. Безпека країни складається з безпеки її структурних і, насамперед, із безпеки її первинної ланки господарювання. Це майже аксіома. Разом з тим, економічні інтереси держави і її структурних складових не завжди збігаються. Про це свідчить реакція впливу ринкової конкуренції на економіку країни в цілому та економіку окремого підприємства або банка. Для соціально-орієнтованої економіки країни конкуренція є двигуном її розвитку та вдосконалення. І в інтересах держави захистити її всіма можливими засобами. Для окремого підприємства або банка – це «головний біль, боротьба за утримання на плаву» в бурхливому океані підприємницького ризику. Тому ставлення керівництва банку до конкуренції відповідне.

Таким чином, економічна (банківська) безпека з одного банку є складовою частиною системи національної безпеки, поряд з такими її елементами як технічна безпека, енергетична, військова, екологічна, інформаційна та інше.

З іншого боку кожний елемент національної безпеки має економічний аспект. Тобто, тут все взаємопов'язане: не може бути військової чи інформаційної безпеки при неформальній економіці, так як не може бути ефективної економіки, коли суспільство перебуває в стані конфліктів та інформаційних війн.

Як показує розвиток світової фінансової кризи, незважаючи на те, що вона розпочалася в банківському секторі, через невеликий проміжок часу її вплив відчули всі інші галузі економіки. Пояснюється це тим, що на сьогоднішній день існує тісний зв'язок між всіма секторами економіки. Отже особливої уваги потребують методи забезпечення фінансової безпеки, а також науково-методичні підходи до формування комплексної системи безпеки на рівні окремого банку.

Щодо банківської системи України, то в міру входження економіки нашої країни у світову, збільшення ступеня її інтеграції у світову фінансову систему, залежність від нестабільності на світових фінансових ринках зростає. Вплив останніх подій все більше позначається і на банківській системі України. Зокрема, починають виникати проблеми з ліквідністю, зростає вартість ресурсів для банків, згортаються деякі проекти через нестачу фінансових ресурсів і неможливість їх отримання на зовнішніх ринках.

При цьому слід враховувати, що однією з найбільш небезпечних загроз для економіки України є порушення її фінансово-банківської системи. Система, яка складалася, потребує від банківських закладів першочергових заходів по підвищенню рівня своєї діяльності, поліпшення ефективності кредитування, корінної зміни кадрової політики, попередженню посягань кримінальних елементів на кошти банків та їх клієнтів. У цих умовах значно підвищується значення банківських підрозділів, які займаються забезпеченням безпеки та охорони.

На наш погляд без подальшого розвитку вітчизняного стратегічно важливого напрямку – забезпечення безпеки банківської діяльності – можливо просто втратити всю діяльність і ефективність у цій справі тому, що занадто велика кількість публікацій орієнтована на закордонні видання та досвід у цій справі. Практичне використання таких видань у нас неможливе, за розбіжністю необхідних правових баз.

Автори висловлюють глибоку подяку доктору технічних наук, професору (Університет банківської справи, Черкаського інституту банківської справи Національного банку України) Засядько Аліні Анатоль'ївні, доктору економічних наук, професору (Львівський державний університет внутрішніх справ) Живко Зінаїді Богданівні, доктору юридичних наук, професору Шакуну Василію Івановичу (Київська академія внутрішніх справ) за уважне та доброзичливе рецензування, висловлені зауваження та поради, які сприяли значному поглибленню та покращенню видання. Автори сподіваються, що їх робота зможе допомогти у процесі організації, функціонування та захисту банківської інформації.

ГЛАВА І
МЕТОДИ ТА ЗАДАЧІ ЗАБЕЗПЕЧЕННЯ БАНКІВСЬКОЇ БЕЗПЕКИ

Безпека банку – це його стан захищеності від зовнішніх та внутрішніх загроз, який дозволяє надійно зберегти та ефективно використовувати фінансовий, матеріальний та кадровий потенціал.

Забезпечення безпеки банку – це діяльність його посадовців, спеціального підрозділу власної безпеки, державних правоохоронних органів та інших структур, спрямована на запобігання можливого порушення його нормального функціонування. Ціллю забезпечення безпеки банку є захист його власності та працівників від зовнішніх та внутрішніх загроз безпеці, запобігання правопорушень, негативних проявів та виникнення надзвичайних ситуацій.

Вказана ціль досягається тільки при її системній реалізації. При цьому, під системою забезпечення безпеки розуміється комплекс правових, організаційно-керівних, спеціальних, соціально-психологічних, режимних, технічних, профілактичних та пропагандиських мір, спрямованих на якісну реалізацію захисту банку від зовнішніх та внутрішніх загроз для його безпеки та діяльності.

Крім того, необхідно враховувати, що динамічне формування, глобалізація та дедалі більша відкритість телекомунікаційних і комп'ютерних мереж, швидкий розвиток інформаційних технологій, продуктів та послуг створюють принципово нові можливості для економічної та банківської співпраці, обміну інформацією.

Разом з цим, зростає кількість загроз, поширюються злочини в сфері комп'ютерної інформації, так звані "кіберзлочини", загострюється проблема захисту інформації у банківській справі, яка в сучасних умовах визначається наступними чинниками високими темпами зростання парку засобів обчислювальної техніки і зв'язку, розширення областей використання ЕОМ;

– залученням в процес інформаційної взаємодії все більшого числа людей і організацій;

– підвищенням рівня довіри до банківських систем управління і обробки інформації;

– ставленням до інформації, як до товару;

– концентрацією великих обсягів інформації різного призначення і приналежності на електронних носіях;

– наявністю інтенсивного обміну інформацією між учасниками цього процесу;

– кількісним і якісним вдосконаленням способів доступу користувачів до інформаційних ресурсів;

– диференціацією рівнів втрат (збитків) від знищення, модифікації, витоку або незаконного блокування інформації;

– різноманіттям видів загроз і можливих каналів несанкціонованого доступу до інформації;

– зростанням числа кваліфікованих користувачів ЕОМ і можливостей по створенню ними програмно-технічних впливів на банківські системи;

– переходом до ринкових відносин, з властивою їм конкуренцією і різними видами розвідки.

Враховуючи провідну роль комп'ютеризації у банківській справі в Україні та підвищення рівня зацікавленості кримінальних осіб та структур в доступі до банківських систем, виняткової актуальності набуває попередження таких правопорушень.

В усіх аспектах проблеми захисту інформації в банківській справі основним елементом є аналіз усіх ймовірних загроз, яким піддається банківська система.

Під загрозою інформації що обробляється в автоматизованій системі мається на увазі будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації чи нанесення збитків автоматизованій системі (АС) тобто: порушення конфіденційності, цілісності та доступності інформації.

Загрози інформації в автоматизованих банківських системах можна розподілити на два класи:

– об'єктивні (природні), що характеризуються впливом на об'єкт захисту фізичних процесів або стихійних природних явищ, які не залежать від людини;

– суб'єктивні, пов'язані з діяльністю людини. Серед останніх можливо виділити:

– ненавмисні, викликані помилковими діями співробітників і відвідувачів банків;

– навмисні, що є результатом навмисних дій порушників. Навмисні загрози можуть виникати як зсередини системи (з боку учасників процесу обробки інформації), так і ззовні (з боку сторонніх осіб).

Навмисні загрози банківській справі є найбільш численними у класифікації видів загроз. До їх переліку слід віднести:

– проникнення у систему через комунікаційні канали зв'язку з присвоєнням повноважень легального користувача з метою підробки, копіювання або знищення інформації. Реалізується розпізнаванням або підбором паролів і протоколів, перехопленням паролів при негласному підключенні до каналу зв'язку під час сеансу, дистанційним перехопленням паролів у результаті отримання та обробки побічного електромагнітного випромінювання;

– проникнення у систему через комунікаційні канали зв'язку при перекомунікації каналу на модем порушника після входження легального користувача в мережу й пред'явлення ним своїх повноважень з метою присвоєння прав цього користувача на доступ до інформації;

– копіювання фінансової інформації і паролів при негласному пасивному підключенні до локальної мережі або прийомі побічного електромагнітного випромінювання мережевого адаптеру;

– виявлення паролів легальних користувачів при негласному активному підключенні до локальної мережі при імітації запиту операційної системи мережі;

– аналіз трафіка для виявлення протоколів обміну;

– підключення до каналу зв'язку в ролі активного ретранслятора для фальсифікації платіжних документів, зміни їх змісту, порядку проходження повторної передачі, затримання доставки;

– блокування каналу зв'язку власними повідомленнями, що викликає відмову від обслуговування легальних користувачів;

– відмова абонента від факту прийому (передачі) платіжних документів або створення помилкових відомостей про час прийому (передачі) повідомлень для зняття з себе відповідальності за виконання цих операцій;

– створення помилкових стверджень про отримання (передачу) платіжних документів;

– несанкціонована передача конфіденційної інформації в складі легального повідомлення для виявлення паролів, ключів і протоколів доступу;

– оголошення себе іншим користувачем (маскування);

– зловживання привілеями супервізора для порушення механізмів захисту банківської інформації;

– перехоплення електромагнітного випромінювання від дисплеїв, серверів або робочих станцій для копіювання інформації і виявлення процедур доступу;

– збір і аналіз використаної друкованої інформації, документації та інших матеріалів для копіювання інформації або виявлення паролів, ідентифікаторів, процедур доступу і ключів;

– візуальне перехоплення інформації, виведеної на екрани дисплеїв або вводу з клавіатури для виявлення паролів, ідентифікаторів і процедур доступу;

– негласна перебудова устаткування або програмного забезпечення з метою впровадження засобів несанкціонованого доступу до інформації (програм-перехоплювачів і «троянських коней», апаратури аналізу інформації тощо), а також знищення інформації або устаткування (наприклад, за допомогою програм–вірусів, ліквідаторів із дистанційним управлінням тощо);

– знищення інформації або створення збоїв в комп'ютерній системі за допомогою вірусів для дезорганізації діяльності банку. Реалізується шляхом внесення вірусів у систему в неробочий час, підміни ігрових програм, або користування співробітником банку «подарунком» у вигляді нової комп'ютерної гри;

– викрадення магнітних носіїв з метою одержання доступу до даних та програм;

– знищення устаткування, магнітних носіїв або дистанційне знищення інформації;

– зчитування інформації з жорстких і гнучких дисків (у тому числі залишків «стертих» файлів), магнітних стрічок при копіюванні даних з устаткування на робочих місцях у неробочий час;

– копіювання даних з терміналів, залишених без нагляду в робочий
час;

– копіювання даних з магнітних носіїв, залишених на столах або в комп'ютерах, шафах тощо;

– копіювання даних з устаткування і магнітних носіїв, прибраних у спеціальні сховища;

– внесення змін у дані і програми для підробки і фальсифікації фінансових документів в результаті негласного відвідування у неробочий час;

– використання залишеного без нагляду устаткування у робочий час;

– внесення змін у дані, записані на залишених без нагляду магнітних носіях;

– встановлення прихованих передавачів для виведення інформації або паролів з метою копіювання даних або доступу до них по легальних каналах зв'язку з комп'ютерною системою в результаті негласного відвідування у неробочий час;

– підміна елементів устаткування, що залишені без нагляду у робочий час;

– встановлення ліквідаторів уповільненої дії або з дистанційним управлінням (програмних, апаратних або апаратно-програмних);

– внесення змін або зчитування інформації у базах даних або окремих файлах через присвоєння чужих повноважень у результаті добору паролів з метою копіювання, підробки або знищення фінансової інформації;

– виявлення паролів при викраденні або візуальному спостереженні;

– використання програмних засобів для подолання захисних можливостей системи;

– використання включеного в систему термінала, залишеного без нагляду;

– несанкціоноване перевищення своїх повноважень на доступ або повноважень інших користувачів в обхід механізмів безпеки (наприклад, негласне вилучення магнітних носіїв з наступним поверненням для копіювання, підробки або знищення даних);

– вилучення інформації із статистичних баз даних у результаті використання семантичних зв'язків між таємною та нетаємною інформацією з метою добування конфіденційних відомостей.

За частотою прояву навмисні загрози можна розташувати у такій послідовності:

– копіювання і викрадення програмного забезпечення;

– несанкціоноване введення даних;

– зміна або знищення даних на магнітних носіях;

саботаж;

– викрадення інформації;

– несанкціоноване використання ресурсів комп'ютерів;

– несанкціоноване використання банківський несанкціонований доступ до інформації високого рівня таємності. Реалізація навмисних загроз в цілому може призвести до

– безпосереднього розкриття або зміни даних. Дії порушника можна розподілити на чотири основних категорії:

– знищення інформації – необоротна модифікація інформації, наприклад, знищення даних на диску;

– модифікація інформації (порушення цілісності інформації) – зміна користувачем або процесом інформації, що міститься в об'єкті, наприклад: зміна програм обробки, даних тощо;

– блокування інформації – дії, в наслідок яких унеможливлюється доступ до інформації, наприклад: неможливість використання інформації, тобто припинення доступу до інформації користувачам;

– виток інформації – результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним або юридичним особам, що не мають права доступу до неї, наприклад: зчитування, перехоплення або копіювання інформації з метою одержання даних, що можуть бути використані порушником або третьою стороною.

Особливу небезпеку становить безконтрольне завантаження програмного забезпечення ЕОМ, у якому можуть бути змінені дані, алгоритми або введена програма «троянський кінь» - програма, яка, будучи авторизованим процесом, окрім виконання документованих функцій, здатна здійснювати приховані дії від особи авторизованого користувача в інтересах розробника цієї програми, наприклад, програма, що виконує додаткові незаплановані функції: запис інформації на сторонній носій, передачу в канали зв'язку іншого абонента обчислювальної мережі, занесення в систему комп'ютерного вірусу тощо.

Як висновок, необхідно зазначити, що суб'єктами злочинних дій у банківський справі можуть бути співробітники банку (працюючі або колишні), клієнти банку, конкуренти або конкуренти клієнтів банку та співробітники державних органів. Специфіка побудови банківських систем, с точки зору їх уразливості, пов'язана в

основному з наявністю інтенсивної інформаційної взаємодії між територіально рознесеними і різнорідними (різнотипними) елементами.

Вразливими є буквально всі основні структурно-функціональні елементи розподілених банківських систем і робочі станції, сервери, міжмережеві мости, канали зв'язку.

Тому, ефективно побудована система захисту інформації - важлива складова успішного проведення аналізу ризику і визначення вимог до складу і характеристик системи захисту, що забезпечує надійну і ефективну протидію зловмиснику.

Така система повинна забезпечувати вирішення цілого комплексу задач:

– захист законних прав та інтересів банка, як суб'єкта економічної діяльності його працівників;

– збір, оцінка та прогнозування даних, які характеризують обстановку навколо банку та в ньому самому;

– вивчення партнерів, клієнтів та конкурентів;

– своєчасне виявлення інтересу до банку та його співробітників з боку сил або осіб, які можуть стати джерелом загроз безпеці;

– запобігання проникненню в банк суб'єктів економічного шпигунства, організованої злочинності та окремих осіб з протиправними намірами;

– протидію технічному проникненню у банк зі злочинними намірами;

– попередження та припинення можливої протиправної та іншої негативної діяльності співробітників банку щодо скоєння шкоди його безпеці;

– захист працівників банку від насильних посягань;

– охорону фінансових та матеріальних цінностей, а також відомостей, що є комерційною таємницею банку;

– здобуття необхідної інформації щодо прийняття правлінням банку оптимальних управлінських рішень з питань стратегії та тактики фінансової та іншої діяльності;

– фізичну та технічну охорону будинків, споруд, території та транспортних засобів банка;

– формування у засобах масової інформації, у партнерів та клієнтів сприятливої думки щодо банка, яка підтримує здатність у реалізації його планової діяльності;

– створення умов щодо відшкодування матеріальних та моральних збитків, що завдані банку та його співробітникам неправомірними діями організацій або окремих осіб;

– контроль ефективності функціонування системи безпеки. Система забезпечення безпеки банку будується на основі дотримання принципів:

– законності;

– поважання прав та свобод громадян;

– централізованого керування;

– координації та взаємодії з державними правоохоронними органами;

– самостійності та відповідальності;

– розумної достатності, відповідно реальним загрозам безпеки;

– застосування надсучасного матеріально-технічного оснащення;

– стимулювання суб'єктів системи;

– компетентності;

– конфіденційності;

– комплексного використання сил та засобів.

Легко помітити, який численний перелік задач та принципів побудови і функціонування має система що розглядається. Наведені вище обставини свідчать про складність і великий обсяг відповідної роботи та велику відповідальність, з якою до неї слід підходити.

Надійність та ефективність функціонування систем безпеки також оцінюється по багатьом критеріям:

– відсутність спроб (своєчасне виявлення) несанкціонованого проникнення у банк із злочинною метою;

– відсутність фактів (недопущення) витоку інформації, розголошення відомостей, які є комерційною таємницею банку;

– відсутність (попередження) протиправних та негативних дій з боку співробітників банку;

– збереження фінансових та матеріальних цінностей банку та його співробітників;

– припинення спроб насильних посягань на життя та здоров'я співробітників банку;

– попередження надзвичайних ситуацій.

Головним, інтегруючим критерієм можна вважати стабільність функціонування та розвиток банку у відповідності з його планами та задачами у сучасних важких умовах.

В забезпеченні безпеки банку повинні бути задіяні наявні сили та засоби. Організація та виконання даної функції покладаються на спеціально створений підрозділ, працівники якого можуть бути штатними спеціально підготовленими співробітниками банку. Кількісне співвідношення персоналу банка та співробітників підрозділу безпеки визначається керівництвом банку в залежності від обставин, обстановки та передбаченого обсягу роботи. Підрозділ безпеки для реалізації покладених на нього завдань, забезпечується необхідними технічними, матеріальними та фінансовими засобами.

Процес забезпечення безпеки банку повинен базуватися на використанні доступних, найсучасніших засобів захисту від протиправних посягань.

Поняття інформаційної безпеки банку

Словосполучення "інформаційна безпека" у різних контекстах може мати різне значення.

У даному підручнику наша увага буде зосереджена на зберіганні, обробці та передачі інформації незалежно від того, якою мовою (українською чи якою-небудь іншою) вона закодована, хто або що є її джерелом та який психологічний вплив вона має на людей. Тому термін "інформаційна безпека" використовується у вузькому змісті, так, як це прийнято, наприклад, в англомовній літературі.

Під інформаційною безпекою ми будемо розуміти захищеність інформації й інфраструктурою, яка її підтримує від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати неприйнятної шкоди суб'єктам інформаційних відносин, у тому числі власникам і користувачам інформації й підтримуючої інфраструктури. (Далі ми пояснимо, що варто розуміти під підтримуючою інфраструктурою.)

Захист інформації – це комплекс заходів, спрямованих на забезпечення інформаційної безпеки.

Таким чином, правильний з методологічної точки зору підхід до проблем інформаційної безпеки починається з виявлення суб'єктів інформаційних відносин й інтересів цих суб'єктів, пов'язаних з використанням банківських систем (БС). *Загрози інформаційної безпеки* – це зворотний бік використання інформаційних технологій. Із цього положення можна вивести два важливих висновки:

1. Трактування проблем, пов'язаних з інформаційною безпекою, для різних категорій суб'єктів може істотно розрізнятися. Для, ілюстрації досить зіставити режимні державні організації й банківські структури. У першому випадку «нехай краще все зламається, ніж ворог довідається хоч один секретний біт», у другому – «наші секрети належать нам, аби тільки все працювало»

2. Інформаційна безпека не зводиться винятково до захисту від несанкціонованого доступу до інформації, це принципово більш широке поняття. Суб'єкт інформаційних відносин може постраждати (зазнати збитків й/або одержати моральний збиток) не тільки від несанкціонованого доступу, але й від поломки системи, що викликала перерву в роботі. Більше того, для багатьох банків власне захист від несанкціонованого доступу до інформації стоїть по важливості на першому місці.

Повертаючись до питань термінології, відзначимо, що термін "комп'ютерна безпека" (як еквівалент або замінник ІБ) видається нам занадто вузьким. Комп'ютери – тільки одна зі складових інформаційних систем, і хоча наша увага буде зосереджена в першу чергу на інформації, що зберігається, обробляється й передається за допомогою комп'ютерів, її безпека визначається всією сукупністю складових й, у першу чергу, найслабшою ланкою, якою в переважній більшості випадків є людина, яка (написала, наприклад, свій пароль на "гірчичнику", наклеєному на монітор).

Відповідно до визначення інформаційної безпеки, вона залежить не тільки від комп'ютерів, але й від інфраструктури, яка її підтримує, до якої можна віднести системи електро-, водо- і теплопостачання, кондиціонери,

засоби комунікацій і, звичайно, обслуговуючий персонал. Ця інфраструктура має самостійну цінність, але нас цікавити не лише те, як вона впливає на виконання інформаційною системою запропонованих їй функцій.

Звернемо увагу, що у визначенні ІБ перед іменником "збиток" стоїть прикметник "неприйнятний". Вочевидь, застрахуватися від усіх видів збитків неможливо, тим більше неможливо зробити це економічно доцільним чином, коли вартість захисних засобів і заходів не перевищує розмір очікуваного збитку. Виходить, із чимось доводиться миритися й захищатися потрібно тільки від того, з чим змиритися ніяк не можна. Іноді таким неприпустимим збитком є нанесення шкоди здоров'ю людей або стану навколишнього середовища, але частіше поріг неприйнятності має матеріальне (грошове) вираження, а метою захисту інформації стає зменшення розмірів збитків до припустимих значень.

Основні складові інформаційної безпеки банку

Інформаційна безпека – багатогранна, можна навіть сказати, багатомірна область діяльності, у якій успіх може принести лише систематичний, комплексний підхід.

Спектр інтересів суб'єктів, пов'язаних з використанням інформаційних систем, можна розділити на наступні категорії: забезпечення доступності, цілісності й конфіденційності інформаційних ресурсів і підтримуючої інфраструктури.

Іноді в сукупність основних складових ІБ включають захист від несанкціонованого копіювання інформації, але, на наш погляд, це занадто специфічний аспект із сумнівними шансами на успіх, тому ми не будемо його виділяти.

Пояснимо поняття доступності, цілісності й конфіденційності.

Доступність – це можливість за прийнятний час одержати необхідну інформаційну послугу.

Під *цілісністю* мається на увазі актуальність і несуперечність інформації, її захищеність від руйнування й несанкціонованої зміни.

Нарешті, *конфіденційність* – це захист від несанкціонованого доступу до інформації.

Інформаційні системи створюються (купуються) для одержання певних інформаційних послуг. Якщо з тих або інших причин надати ці послуги користувачам стає неможливо, це, мабуть, завдає шкоди всім суб'єктам інформаційних відносин. Тому, не протиставляючи доступність іншим аспектам, ми виділяємо її як найважливіший елемент інформаційної безпеки.

Особливо яскраво провідна роль доступності виявляється в різного роду системах керування – виробництвом, транспортом і т.п. Зовні менш драматичні, але також досить неприємні наслідки – і матеріальні, і моральні – може бути тривала недоступність інформаційних послуг, якими користується велика кількість людей (продаж залізничних та авіаквитків, банківські послуги й т.п.).

Цілісність можна підрозділити на статичну (що розуміється як незмінність інформаційних об'єктів) і динамічну (яка стосується коректного виконання складних дій (транзакцій). Засоби контролю динамічної цілісності застосовуються, зокрема, при аналізі потоку фінансових повідомлень із метою виявлення крадіжки, передвпорядкування або дублювання окремих повідомлень.

Цілісність виявляється є найважливішим аспектом ІБ у тих випадках, коли інформація стає "керівництвом до дії". Рецептура ліків, запропоновані медичні процедури, набір і характеристики комплектуючих виробів, хід технологічного процесу все це приклади інформації, порушення цілісності якої може виявитися в буквальному значенні смертельним. Неприємно й перекручування офіційної інформації, будь-то текст закону або сторінка Web-сервера якої-небудь урядової організації.

Конфіденційність – найпроблемніший у нас у країні аспект інформаційної безпеки. На жаль, практична реалізація засобів по забезпеченню конфіденційності сучасних інформаційних систем натрапляє в Україні на серйозні труднощі. По-перше, відомості про технічні канали витоку інформації є закритими, так що більшість користувачів позбавлені можливості скласти

уявлення про потенційні ризики. По-друге, на шляху використовуваної криптографії як основного засобу забезпечення конфіденційності стоять численні законодавчі перепони й технічні проблеми.

Якщо повернутися до аналізу інтересів різних категорій суб'єктів інформаційних відносин, то майже для всіх, хто реально використовує ІС, на першому місці стоїть доступність. Практично не поступається їй по важливості цілісність – який сенс в інформаційній послузі, якщо вона містить перекручені відомості?

Нарешті, конфіденційні моменти є також у багатьох організацій (навіть у згадуваних вище навчальних інститутах намагаються не розголошувати відомості про зарплату співробітників) і окремих користувачів (наприклад, паролі).

Основні завдання фінансової безпеки банків та фактори, що впливають на неї

Ключові характеристики фінансової безпеки банків:

– забезпечує рівноважний і стійкий фінансовий стан банку;

– сприяє ефективній діяльності банку;

– дозволяє на ранніх стадіях визначити проблемні місця в діяльності банку;

– нейтралізує кризи і запобігає банкрутствам.

Враховуючи дослідження які наведені в літературі [2,3,30], можна зробити висновок про те, що основна мета фінансової безпеки банку полягає в безперервній і стійкій підтримці стану, який характеризується збалансованістю і стійкістю до впливу зовнішніх і внутрішніх загроз [2, 30].

Проведений аналіз наукових робіт [4] показав, що фінансова безпека банку визначається:

– стабільністю і стійкістю фінансового стану банку;

– ступенем ефективності фінансово-економічної діяльності;

– рівнем контролю за зовнішніми і внутрішніми ризиками;

– рівнем достатності власного капіталу;

– ступенем захищеності інтересів акціонерів.

Забезпечення фінансової безпеки банків передбачає виконання таких завдань:

– ідентифікацію ризиків і пов'язаних з ними потенційних небезпек;

– визначення індикаторів фінансової безпеки банку;

– впровадження системи діагностики та моніторингу стану фінансової безпеки;

– розробку заходів, спрямованих на забезпечення фінансової безпеки банку як в короткостроковому, так і в довгостроковому періодах;

– контроль за виконанням запланованих заходів;

– аналіз виконання заходів, їх оцінка, корегування;

– ідентифікацію загроз банку і корегування індикаторів залежно від зміни стану зовнішнього середовища, цілей і завдань банку.

У цілому загрози безпеці банків можна поділити на дві великі групи – внутрішні й зовнішні. До зовнішніх належать загрози, що містять у собі фактори, які є результатом впливу зовнішнього середовища на банк, зокрема діяльність держави, економічна кон'юнктура в країні та світі, конкуренти та ін. До внутрішніх загроз належать фактори, які або безпосередньо генеруються банком, або є частиною його внутрішнього середовища. До основних внутрішніх загроз можна віднести рівень забезпеченості фінансовими ресурсами, незадовільну структуру активів і пасивів, некомпетентність вищого керівництва і персоналу, а також інші фактори, що безпосередньо належать до внутрішньої діяльності банку.

Перелік внутрішніх і зовнішніх загроз банку наведений в табл.1.1.,1.2.

Таблиця 1.1.

Основні види внутрішніх загроз

№	Внутрішні загрози	Можливі прояви
1.	Якість кредитного портфеля	– рівень проблемних кредитів; – неповернення кредитів; – незбалансована кредитна політика; – збільшення простроченої заборгованості
2.	Рівень і компетенція менеджменту	– прийняття неправильних управлінських рішень; – неефективна діяльність внаслідок неоптимального використання потенціалу банку; – помилки в стратегічному плануванні й

		прогнозуванні; – побудова нераціональної структури банку
3.	Структура активів і пасивів	– дефіцит власних коштів; – низькій рівень ліквідності й нестача ліквідних активів; – завищений рівень ризикових актів; – збільшення активів низької якості; – нестачу капіталу; – незбалансованість активів і пасивів за строками
4.	Залежність від інсайдерів	– пільгове кредитування засновників; – прийняття управлінських рішень під тиском власників; – відстоювання інтересів власників, а не інтересів банку
5.	Злочинні дії персоналу	– шахрайство; – розголошення конфіденційної інформації; – неефективна робота персоналу; – перехід ключових працівників до конкурентів; – недостатній рівень кваліфікації персоналу
6.	Неефективна діяльність банку	– низький рівень прибутків; – недосконала оцінка кредитних ризиків; – низький рівень прибутковості активів; – слабке маркетингове дослідження ринку і як наслідок недостатній рівень диверсифікованості банківських операцій

Таблиця 1.2.

Основні види зовнішніх загроз

№ п/п	Зовнішні загрози	Можливі прояви
1.	Нормативне регулювання банківської діяльності	– недосконаліть законодавства, наприклад, відсутність закону про банківську таємницю створює загрозу розголошення інформації про діяльність банку та його клієнтів; – мінливість законодавства; – відкликання ліцензії на здійснення банківської діяльності або зміна умов ліцензування.
2.	Грошово-кредитна політика центрального банку	– ставка обов'язкового резервування; – обсяги рефінансування й розмір облікової ставки; – обсяг пропозиції грошей в обігу; – зміна облікової ставки; – обсяг операцій з ОВДП
3.	Нестабільність зовнішнього середовища	– глобальні або локальні фінансові кризи; – неможливість одержати доступ до зовнішніх фінансових ресурсів; – валютний, процентний і ринковий ризики; – блокування активів банку в іншій державі; – державний дефолт.

Продовження таблл.1.1.

4.	Недовіра до банківської системи	– недовіра з боку інвесторів; – недовіра з боку підприємств (кредиторів); – недовіра з боку населення (вкладників); – швидке вилучення великого обсягу коштів із банку; – використання засобів масової інформації для провокування банківської кризи; – погіршення репутації банку; – банкрутство великого банку;
5.	Конкурентне середовище	– не конкурентоспроможність банку; – несумлінна діяльність конкурентів; – різке збільшення ринкових ставок за депозитами; – різке зниження ринкових ставок за кредитами; – завдання економічних збитків підприємствам; – ключовим контрагентам банку.
6.	Злочинна діяльність	– шахрайські дії третіх осіб; грабіж і крадіжка цінностей банку; злом комп'ютерних мереж банку; рейдерські атаки на банк; махінації з акціями банку.
7.	Негативні макроекономічні умови	– високий рівень інфляції та інфляційних очікувань; – дефіцит інвестиційних коштів і низькій рівень інвестиційної активності в країні; – економічна криза в країні; – падіння попиту на кредити й банківські послуги.
8.	Діяльність держави	– нестабільність податкової, кредитної й страхової політики; – політична нестабільність; – військові конфлікти.

Основні загрози безпеки банків

Рівень і інтенсивність злочинів відносно банківських структур свідчать про недостатню обізнаність служб безпеки про процеси, що відбувається як усередині банків, так і в середовищі їх функціонування. Для обліку особливостей і тенденцій кримінальної дії слід постійно здійснювати кримінологічний моніторинг.

Слід звернути особливу увагу найбільш просторові і небезпечні види – «напрями головного удару» злочинного середовища. Це:

– проникнення, в кредитно-фінансові утворення груп шахраїв (у тому числі міжнародного масштабу), що мають легальне комерційне прикриття і здійснюють розкрадання з використанням підроблених платіжних документів;

– здирства з боку правоохоронних і контролюючих органів, державних органів, розміщуючи інвестиції і державні замовлення;

– розкрадання кредитів;

– усунення конкурентів з використанням правоохоронних органів засобів масової інформації.

Для організації і діяльності служби безпеки необхідно враховувати тенденції в злочинній активності. Назвемо основні з них, характерні для злочинності в цілому:

– легалізація організованих злочинних груп (утворення комерційних структур для відмивання доходів);

– посилення агресивних мотивів поведінки, збільшення кількості актів терору відносно банків;

– розширення криміногенного середовища за рахунок безробітних, дрібних торгівців, біженців і молоді;

– збільшення кількості фактів шахрайства в громадсько-правових стосунках;

– поширення кримінальних способів рішення будь-яких, у тому числі цивільно-правових, конфліктів (наприклад, повернення кредитів);

– «опіка» банківських структур з боку посадовців державного апарату;

– примус їх до корупційних зв'язків і фінансових махінацій;

– використання в конкурентній боротьбі неправомірних дій з боку «дружніх правоохоронних і інших державних органів, а також дискредитаційних компаній;

– зростаюча озброєність злочинних угрупувань.

Говорячи про тенденції специфічній злочинною активності, пов'язаною з кредитно-фінансовою сферою, необхідно відмітити посилення позицій організованих злочинних груп (ОЗГ), що займаються «вибиванням грошей», у боржників під прикриттям фірм з числа колишніх співробітників МВС, КГБ, СБУ та податкової міліції;

– інтенсивною дією з боку загальнокримінальної злочинності.

Комерційні банки є пріоритетними об'єктами для здійснюваних злочинних посягань, таких, як:

– примус посадовців банку до змови;

– розкрадання конфіденційної інформації, що стосується кредитуванню;

– тиск за замовленням конкуруючих організацій;

– створення для співробітників банків ситуацій, які згодом використовуються для шантажу;

– впровадження членів ОЗГ у банківські структури;

– організація банкрутства або ліквідації комерційного банку шляхом дискредитації, ініціації фінансової паніки і затребування депозитів вкладниками (з використанням користувача «замовлених» статей). Слід

зазначити все більше поширення злочинних дій «ділового», «ринкового» характеру: повідомлення неправдивих відомостей про учасників угоди, що спотворюють їх правомочність на укладання ділових угод; використання, що неповної інформації при реєстрації підприємства; підміна контрагента, що бере участь в угоді; здійснення прихованого посередництва та ін.