ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КАФЕДРА УПРАВЛІННЯ ФІНАНСОВО-ЕКОНОМІЧНОЮ БЕЗПЕКОЮ І ПРОЕКТАМИ

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ДО ПРАКТИЧНИХ ЗАНЯТЬ

з дисципліни

«ОРГАНІЗАЦІЯ ТА УПРАВЛІННЯ ФІНАНСОВО-ЕКОНОМІЧНОЮ БЕЗПЕКОЮ БАНКІВ ТА ФІНАНСОВИХ УСТАНОВ»

Запоріжжя

Розділ І. Сутність системи фінансово-економічної безпеки банків та фінансових установ

Тема 1. Основи організації та управління фінансово-економічною безпекою фінансових та банківських установ

Питання для обговорення:

1. Сили та засоби безпеки фінансових та банківських установ.
2. Концепція безпеки фінансових та банківських установ.
3. Види безпеки.
4. Заходи фінансово-економічної безпеки.
5. Забезпечення функціонування системи заходів фінансово-економічної безпеки.

Методичні рекомендації:

Питання 1. Сили та засоби безпеки фінансових та банківських установ

При вивченні цього питання необхідно звернути увагу на те, що виконання заходів безпеки забезпечується через діяльність сил безпеки і використання різноманітних засобів. Залежно від способу організації безпеки її силами виступають: підрозділи безпеки банків, спеціалізовані фірми, організації, які надають банкам послуги безпеки, персонал банків. До засобів безпеки відносяться технічні засоби охорони, програмні й технічні засоби захисту інформації, спеціальні засоби і техніка, інженерно-технічні засоби обмеження доступу, засоби зв'язку, обробки і передавання інформації та інше обладнання і техніка, які використовуються для забезпечення ефективної реалізації заходів безпеки.

Слід зазначити, що безпека діяльності банків, як й інших комерційних структур, забезпечується всіма їх підрозділами і працівниками. Вона не може бути ефективною, якщо нею буде займатись якийсь один, хай навіть найпрофесійніший, підрозділ або фахівець.

Практична реалізація заходів безпеки може бути організована: укладанням договорів із державними органами охорони, приватними охоронними та детективними фірмами (на повне або часткове здійснення заходів безпеки); створенням власного підрозділу безпеки.

Запитання для самоперевірки:

1. Що відноситься до сил безпеки фінансових та банківських установ?
2. Що відноситься до засобів безпеки фінансових та банківських установ?
3. Яким чином створюються підрозділи безпеки в банку?

Питання 2. Концепція безпеки фінансових та банківських установ

Вивчаючи це питання варто зазначити, що безпека банку забезпечується на основі принципу централізованого управління стратегічними напрямками даної діяльності на рівні керівництва банку. Крім того, основними принципами банківської безпеки є:

законність: заходи, які забезпечують безпеку банку, базуються на чинних законах України, постановах Кабінету Міністрів, указах Президента України, нормативних актах Національного банку, вимогах документів місцевих органів влади та статуту банку;

самостійність і відповідальність: підрозділи безпеки банку повинні мати у своєму розпорядженні всі необхідні засоби для ефективного розв'язання поставлених перед ними завдань, повноваження осіб і підрозділів банківської безпеки суворо регламентуються нормативними актами банків;

економічна доцільність: заходи безпеки не повинні призводити до погіршення умов діяльності та стану банку, перешкоджати реалізації його інтересів; витрати на проведення заходів безпеки мають бути адекватними ефективності останніх;

компетентність: виконання заходів безпеки повинно здійснюватися грамотно, на високому професійному рівні, базуватися на об'єктивних даних, не обмежувати права і не ображати гідності громадян;

цілеспрямованість: заходи безпеки здійснюються у суворій відповідності до завдань, які вирішує банк і виконуються згідно з затвердженою його керівництвом комплексною програмою безпеки;

координація і взаємодія: служба безпеки банку координує зусилля всіх його установ і підрозділів щодо виконання заходів безпеки; з цією метою встановлює необхідні зв'язки з підрозділами банку і зовнішніми організаціями;

конфіденційність: усі заходи безпеки проводяться на конфіденційній основі, без їх розголошення; про результати виконання заходів безпеки інформується керівництво банку і за його рішенням інші особи, робота яких пов'язана з необхідністю володіння відповідною інформацією.

Надійність та ефективність безпеки визначаються через реалізацію відповідних вимог, якими є: безперервність, плановість, конкретність, активність, універсальність, комплексність.

Запитання для самоперевірки:

1. Опишіть концепцію безпеки фінансових та банківських установ.
2. Перерахуйте і поясніть основні принципи банківської безпеки.

Питання 3. Види безпеки

При вивченні даного питання, необхідно усвідомити, що вид безпеки — це сукупність ознак, які характеризують готовність банку протистояти загрозам його діяльності.

Серед видів безпеки банку можна виділити:

особисту безпеку - здатність кожного працівника банку протистояти загрозам його здоров'ю, життю і професійній діяльності на основі оволодіння нормами і правилами безпечної поведінки. Досягається дотриманням усіма працівниками заходів застереження, проведенням спеціальних охоронних заходів щодо працівників банку; вивченням кожним працівником правил поведінки у складних умовах та екстремальних ситуаціях, грамотними діями в них;

колективну безпеку - здатність підрозділів банку забезпечувати ефективний режим роботи в умовах дії різноманітних дестабілізуючих факторів. Досягається створенням доброзичливої, спокійної обстановки у колективах, дотриманням принципів справедливості, грамотним стимулюванням праці; постійним вивченням психологічної обстановки в колективах, своєчасним виявленням підвищеної напруженості у взаємовідносинах працівників, попередженням і швидким вирішенням конфліктних ситуацій; виконанням режимних заходів, охороною території, будівель і приміщень; постійною перевіркою стану будівель і обладнання, проведенням атестації приміщень, виконанням протипожежних заходів;

економічну безпеку - стан, за якого забезпечується економічний розвиток і стабільність діяльності банку, гарантований захист його фінансових і

матеріальних ресурсів, здатність адекватно і без істотних втрат реагувати на зміни внутрішньої і зовнішньої ситуації. Досягається створенням ефективного комплексу заходів захисту електронної системи платежів банку і попередження відпливу коштів шляхом фальсифікації фінансових документів; наявністю відповідних установленим вимогам місць зберігання готівки, цінностей, технічних засобів, транспорту та обладнання банку, вмілою їх експлуатацією; грамотною організацією охорони та режимних заходів у банку; створенням обстановки бережливого ставлення до майна банку, суворої і неминучої відповідальності за крадіжки матеріальних засобів та їх псування; ефективним плануванням заходів і дотриманням правил пожежної безпеки; зваженою політикою керівництва банку в усіх сферах банківської діяльності, що забезпечує виправданий ризик та ефективне вкладання грошей, та іншими заходами;

інформаційну безпеку - стан, за якого забезпечується необхідний рівень інформованості його керівництва, персоналу, а також зовнішнього середовища та ефективний захист усіх видів інформації від зовнішніх і внутрішніх загроз. Досягається організацією збору інформації про внутрішнє і зовнішнє середовище банку, проведенням інформаційно-аналітичного дослідження клієнтів, партнерів та конкурентів, інформаційного аудиту та інформаційного моніторингу в банку, аналітичною обробкою інформації; організацією системи інформаційного забезпечення рішень керівництва банку; визначенням категорій банківської інформації та виробленням відповідних заходів щодо її захисту; дотриманням відповідних режимів діяльності банку; виконанням усіма працівниками банку норм і правил роботи з інформацією; своєчасним виявленням спроб і можливих каналів витоку інформації та його припинення.

Запитання для самоперевірки:

1. Що таке вид безпеки?
2. Перерахуйте і опишіть основні види безпеки фінансових та банківських установ.

Питання 4. Заходи фінансово-економічної безпеки

Вивчаючи це питання, в першу чергу необхідно зрозуміти, що заходи фінансово-економічної безпеки поділяються на:

Заходи загального характеру:

1. Здійснення організаційно-правового впливу на діяльність працівників і клієнтів банку з питань безпеки.
2. Підбір, перевірка і контроль роботи персоналу, розроблення ефективної кадрової політики і програм стимулювання праці.
3. Охорона банку.
4. Організація спеціального діловодства.
5. Захист інформаційних ресурсів банку.
6. Удосконалення технології банківського виробництва, введення в них елементів захисту.
7. Формування позитивного іміджу банку.

8. Планування і забезпечення дій банку в кризових ситуаціях.

9. Забезпечення безпеки споруд і будівель установ банку, їх комунікаційних систем.

10. Створення системи оповіщення банку.

11. Розроблення заходів відповідальності за порушення установлених правил безпеки банківської діяльності.

Спеціальні заходи:

1. Організація і ведення комерційної розвідки, формування інформаційних ресурсів банку.

2. Інформаційно-аналітичні дослідження клієнтів, партнерів і конкурентів банку.

3. Взаємодія з правоохоронними органами з питань забезпечення безпеки діяльності банку.

4. Вживання заходів щодо попередження, виявлення, локалізації актів недобросовісної конкуренції і промислового шпигунства.

5. Проведення службових розслідувань у банку.

6. Вживання заходів щодо дезінформації конкурентів у випадках проведення проти банку актів недобросовісної конкуренції.

7. Вживання заходів щодо недобросовісних клієнтів, боржників і зловмисників з метою відшкодування ними збитків, яких банк зазнав з їх вини.

Запитання для самоперевірки:

1. Назвіть заходи фінансово-економічної безпеки банку загального характеру.

2. Назвіть спеціальні заходи фінансово-економічної безпеки банку.

Питання 5. Забезпечення функціонування системи заходів фінансово-економічної безпеки

Потрібно усвідомити, що практична реалізація заходів безпеки може бути організована: укладанням договорів із державними органами охорони, приватними охоронними та детективними фірмами (на повне або часткове здійснення заходів безпеки); створенням власного підрозділу безпеки.

Підрозділ безпеки у банку створюється відповідно до сфер, напрямку його діяльності, завдань безпеки та форм її організації. Крім того, на структуру підрозділу впливатимуть можливості банку, обсяг операцій, які він проводить, політика керівництва банку щодо організації безпеки. Як варіант, структура підрозділу (служби, управління, департаменту) безпеки може бути такою:

- керівник підрозділу;
- експертна група для оперативного вирішення проблем, що раптово виникають (може складатися з 3-4 працівників, як правило, фахівців у справі юриспруденції та банківських технологій);
- підрозділ охорони (може включати групи: охорони території і об’єктів, інкасації, особистих охоронців, технічних засобів охорони);

– інформаційно-аналітичний підрозділ (може включати групи: збирання інформації, обробки інформації, зв'язків із пресою, технічну);

– підрозділ захисту інформації (може включати групи: режиму; психологічного контролю; зовнішнього захисту - для взаємодії з правоохоронними органами, підрозділами безпеки інших банків, охоронними та детективними фірмами, органами влади; фінансової безпеки; технічну).

Запитання для самоперевірки:

1. Назвіть основні форми реалізації заходів фінансово-економічної безпеки.
2. Яким чином створюється і функціонує підрозділ безпеки у банку?

Тема 2. Загрози банку

Питання для обговорення:

1. Зовнішні загрози, їх характеристика.
2. Джерела зовнішніх загроз, вплив загроз на діяльність банку.
3. Внутрішні загрози та їх характеристика.
4. Заходи захисту банків від зовнішніх та внутрішніх загроз.

Методичні рекомендації:

Питання 1. Зовнішні загрози, їх характеристика

Економічні загрози можуть реалізовуватись у формі корупції, шахрайства, недобросовісної конкуренції, використання банками неефективних технологій банківського виробництва. Реалізація таких загроз веде до заподіяння збитків банкам або упущення ними вигоди.

Фізичні загрози реалізуються у формі крадіжок, пограбувань майна та коштів банків, поломок, виведення із ладу обладнання банків, неефективної його експлуатації. Унаслідок реалізації таких загроз завдаються збитки банкам, пов'язані з втратою своєї власності та необхідністю нести додаткові витрати на відновлення засобів виробництва та інших матеріальних засобів.

Інтелектуальні загрози проявляються як розголошення або неправомірне використання банківської інформації, дискредитація банку на ринку банківських послуг, різного роду соціальні конфлікти навколо банківських установ або в них самих. Наслідками реалізації таких загроз можуть бути збитки банків, погіршення їх іміджу, соціальна чи психологічна напруженість навколо установ банків або в їх колективах. Причинами таких загроз, як правило, виступають загострення конкуренції на регіональних ринках банківських послуг, неефективна кадрова політика банків, порушення принципу гласності результатів банківської діяльності, відсутність або низька ефективність заходів інформаційного режиму в банках.

Запитання для самоперевірки:

1. Назвіть та дайте характеристику основним зовнішнім загрозам банківської діяльності.

2. Що є наслідками реалізації таких загроз?

Питання 2. Джерела зовнішніх загроз, вплив загроз на діяльність банку

Зовнішні загрози для безпеки банків, як показує практика, можуть створюватись:

- спецслужбами іноземних держав, пов'язаними з ними особами й організаціями, метою діяльності яких є здобування економічної інформації;
- вітчизняними й іноземними кримінальними елементами і структурами;
- конкурентами;
- засобами масової інформації;
- окремими представниками державних установ;
- приватними детективними фірмами;
- колишніми працівниками банків;
- консультантами та радниками, які не є працівниками банківських установ;
- клієнтами та партнерами;
- контролюючими органами та аудиторськими організаціями;
- стихійними лихами.

Запитання для самоперевірки:

1. Назвіть джерела виникнення зовнішніх загроз банківської діяльності.
2. Який їх вплив на діяльність банку?

Питання 3. Внутрішні загрози та їх характеристика

Варто розуміти, що внутрішні загрози, так як і зовнішні, за спрямованістю і характером впливу на діяльність банків можуть бути економічними, фізичними та інтелектуальними.

Внутрішні загрози здебільшого спричиняються:

- діями працівників банків;
- недосконалими технологіями банківського виробництва та неповним його врегулюванням нормативними актами банків;
- недосконалою системою безпеки банків та захисту їх інформації.

Внутрішні загрози, як правило, обумовлюються наявністю передумов для негативних, протиправних дій персоналу банку, безконтрольним використанням засобів виробництва, порушенням режимів діяльності банку.

Враховуючи, що значна частина внутрішніх загроз реалізується за участі або сприяння персоналу банків, можна вважати, що основним джерелом таких загроз є банківські працівники. Виходячи з цього, внутрішні загрози банкам можуть виникати внаслідок:

- непрофесійних дій працівників банків;
- низького стану виховної та профілактичної роботи в банках;

– недосконалої системи заробітної плати та стимулювання праці персоналу банків;

– порушень правил кадрової роботи, невідповідності кадрової політики умовам роботи банків;

– психологічних і комунікаційних особливостей працівників банків;

– відсутності нормативної бази банків, яка б установлювала режими їхньої діяльності та правила поведінки персоналу;

– низького стану трудової і виробничої дисципліни, слабкої вимогливості керівного складу банків.

Запитання для самоперевірки:

1. Назвіть основні внутрішні загрози банківської діяльності.
2. Назвіть джерела та передумови виникнення внутрішніх загроз.

Питання 4. Заходи захисту банків від зовнішніх та внутрішніх загроз

При вивченні даного питання варто звернути увагу на те, що заходи захисту діяльності банку від зовнішніх та внутрішніх загроз поділяються на кадрові, організаційно-технологічні та інтелектуальні.

Кадрові:

1. Підбір, вивчення, перевірка і вибір працівників банку.
2. Мотивація роботи.
3. Контроль роботи.
4. Попередження і вирішення конфліктних ситуацій у колективах.
5. Робота з працівниками, які звільняються з роботи в банку.
6. Розроблення системи заходів відповідальності за допущені порушення і зловживання.
7. Соціальний контроль окремих категорій працівників банку.

Організаційно-технологічні:

1. Розроблення технологій, які виключають (або ускладнюють) шахрайські дії.
2. Дотримання принципу «чотирьох очей».
3. Періодичні перевірки і ревізії, щорічний контроль і облік.
4. Інформаційно-аналітичні дослідження клієнтів, партнерів і конкурентів, ринку.
5. Категоріювання доступу до грошей, матеріальних засобів, цінностей, інформації, документів банку.
6. Нагляд за функціонуванням заходів захисту.
7. Моніторинг виконання зобов’язань клієнтами і партнерами банку.

Інтелектуальні:

1. Формування у працівників банківського патріотизму.
2. Розроблення і впровадження Кодексу банківського службовця.
3. Розроблення і проведення заходів виховного і профілактичного характеру, навчання працівників протидії шахрайським діям.

Запитання для самоперевірки:

1. Назвіть кадрові заходи захисту діяльності банку.

2. Назвіть організаційно-технологічні заходи захисту діяльності банку.
3. Назвіть інтелектуальні заходи захисту діяльності банку.

Практичне завдання: Розрахунок коефіцієнтів ефективності діяльності банку та показників, що характеризують рівень захищеності банку

Таблиця 2.1 – Вихідні даня ра розрахунок коефіцієнтів ефективності діяльності банку

Назва показника	2011 р.	2012 р.	Темп зміни у % або абсол. зміна	Порогове значення
а) Вихідні дані, тис. грн				
1. Чистий прибуток	24 671,1	28 164,6	114,2	-
2. Середньорічні активи загальні	254 211,0	286 722,0	112,8	-
3. Процентні доходи	60 348,0	59 049,0	97,8	-
4. Процентні витрати	17 100,0	22 044,0	128,9	-
5. Доходи загальні	88 788,0	100 590,0	113,3	-
6. Витрати загальні	64 587,0	72 417,0	112,1	-
7. Комісійні доходи	28 440,0	41 541,0	146,1	-
8. Витрати комісійні	47 484,0	50 373,0	106,1	-
9. Середньорічна чисельність працівників	350	400	114	-
б) Коефіцієнти ефективності				
1. Рентабельність активів, % (ряд. 1 : ряд. 2)	9,7	9,8	+0,1	1,5%
2. Рівень процентної маржи (чиста процентна маржа), % ((ряд.3-ряд.4)/ряд.2)*100%	17,01	12,91	-4,1	5,0%
3. Ефективність роботи банку (коефіцієнт окупності витрат доходами), частка од. (ряд. 5 : ряд. 6)	1,375	1,389	0,014 (101,02%)	>1
4. Ефективність операцій з процентними коштами, частка од. (ряд. 3 : ряд. 4)	3,53	2,68	-0,85 (75,92%)	>1
5. Ефективність комісійної діяльності, частка од. (ряд.7: ряд.8)	0,60	0,82	0,22 (136,70%)	>1
6. Прибуток на одного співробітника (продуктивність праці середньорічного працівника), грн./чол. (ряд. 1 : ряд. 9)	70 489,0	70 411,0	-78,00 (99,89%)	11000 грн. /чол.

Таблиця 2.2 – Вихідні дані та розрахунок показників, що характерізують рівень захищеності банку

Назва показника	2011 р.	2012 р.	Темп зміни у % або абсол. зміна	Порогове значення
а) Вихідні дані, тис. грн				
1. Високоліквідні активи (ГК в касі та на коррах. в НБУ	47485,5	37575,9	79,13	-
2. Поточні пасиви (короткострокові)	85422,3	93422,5	109,37	-
3. Кредитний портфель	108 703,8	136 421,4	125,50	-
4. Прострочені і безнадійні кредити	326,1	272,7	83,60	
5. Величина резервів під кредитні операції	3325,6	3547,3	106,67	-
6. Зобов'язання всього	152 531,1	182 636,1	119,70	-
7. Кредитний портфель	108 703,8	136 421,4	125,50	-
8. Капітал	112 904,1	125 926,2	111,50	-
9. Міжбанківські кредити одержані	14 415,9	46 064,4	319,50	-
10. Видані міжбанківські кредити	46999,2	45380,4	96,56	-
11. Довга (+) відкрита валютна позиція	15520,0	13890,0	89,50	-
б) Коефіцієнти захищеності				
1. Ліквідність (миттєва), частка од. (%) (ряд. 1 : ряд. 2)	0,56	0,40	-0,16 (71,43%)	>20%
2. Коефіцієнт проблемних кредитів, частка од. (%) (ряд. 4 : ряд. 3)	0,03 (або 3,0%)	0,02	(-0,01) 66,67	<5%
3. Коефіцієнт кредитних ризиків, частка од. (ряд. 4 : ряд. 5)	0,098	0,077	-0,021 (78,57%)	<1
4. Коефіцієнт співвідношення кредитів і зобов'язань (коефіцієнт активності використання залучених коштів у кредитний портфель), частка од. (ряд. 7 : ряд. 6)	0,71	0,75	0,04 (105,63%)	0,53-0,90
5. Коефіцієнт достатності капіталу, % ((ряд.8 / (ряд.6+ряд.8))*100%	42,53	40,80	-1,73	>10%

6. Співвідношення виданих і отриманих міжбанківських кредитів, частка од. (ряд. 10 : ряд. 9)	3,26	0,98	-2,28 (30,06%)	Якщо >1,4, то це загроза для кредитної і фінансової стійкості банку
7. Загальна валютна позиція, частка од. (ряд.11 : ряд.8)	0,14	0,11	-0,03 (78,57%)	<30%

Тема 3. Недобросовісна конкуренція та промислове шпигунство в банках

Питання для обговорення:

1. Сутність недобросовісної конкуренції та її прояв у банках.
2. Заходи банку щодо захисту від недобросовісної конкуренції.
3. Сутність промислового шпигунства та його прояв у банках.
4. Заходи банку щодо організації захисту від промислового шпигунства.

Методичні рекомендації:

Питання 1. Сутність недобросовісної конкуренції та її прояв в банках

При вивченні даного питання варто звернути увагу на те, що в конкуренції виявляються методи, не сумісні з заведеними на ринку. Діяльність суб'єктів ринку з використанням таких методів конкуренції прийнято називати недобросовісною конкуренцією.

Метою недобросовісної конкуренції в банківській сфері є прагнення банку-конкурента поліпшити або закріпити своє становище чи здобути перевагу на ринку за рахунок послаблення позицій банків-конкурентів і введення в оману клієнтів.

За таких умов основною метою даного питання є вивчення можливостей банків забезпечувати захист їх діяльності від актів недобросовісної конкуренції і промислового шпигунства, опанування формам і методів протидії таким актам.

Запитання для самоперевірки:

1. Дайте визначення поняттю «недобросовісна конкуренція».
2. Що є метою недобросовісної конкуренції?
3. Назвіть основні форми недобросовісної конкуренції.

Питання 2. Заходи банку щодо захисту від недобросовісної конкуренції

При вивченні даного питання необхідно запам'ятати, що *основними заходами протидії актам недобросовісної конкуренції є:*

1. Вивчення ринків та їх суб'єктів, складання характеристик впливу.

2. Визначення найбільш вірогідних конкурентів і складання прогнозів взаємовідносин з ними.

3. Вибір методів поведінки із суб'єктами ринку, використання ділових зв'язків і партнерів для вироблення компромісних рішень із конкурентами.

4. Створення нормативної бази банків, яка регламентувала б порядок взаємовідносин персоналу з зовнішнім середовищем.

5. Включення до технологій, операцій і угод елементів їх захисту.

6. Ведення комерційної розвідки в середовищі конкурентів.

7. Періодичне оприлюднення результатів своєї діяльності.

8. Створення банківських союзів, асоціацій і вироблення правил відповідних поведінки на ринку, які вкладаються в межі добросовісної конкуренції.

Запитання для самоперевірки:

1. Назвіть основні заходи банку щодо захисту від недобросовісної конкуренції.

2. Які з перерахованих заходів є найбільш ефективними? Чому?

Питання 3. Сутність промислового шпигунства та його прояв в банках

Потрібно запам'ятати, що найбільш несприятливі умови діяльності банку створюються у разі ведення проти нього промислового шпигунства. Такі дії можуть завдати дуже великої шкоди банку. Річ у тім, що основним об'єктом діяльності промислових шпигунів є банківська інформація, особливо та, яка стосується планів розвитку діяльності банків, їхніх технологій, управління тощо. Тобто втрата банками такої інформації або її неправомірне поширення буде значною мірою впливати на економічний стан банків, їх ліквідність і платоспроможність. Тому банки повинні вживати заходів щодо захисту та протидії актам промислового шпигунства, безпосередньо у своїх установах.

Сьогодні практично не існує чіткого визначення поняття «промислове шпигунство». Найбільш повне, з юридичного погляду, визначення дає Міжнародна організація кримінальної поліції (Інтерпол): «… це придбання будь-яким обманним шляхом інтелектуальної власності, яка належить будь-якій юридичній особі і яка була створена або законно придбана цією юридичною особою з метою виробництва, що має або може мати промислову цінність...».

Існує багато різних форм і методів промислового шпигунства. Але, попри їх численність, вони обумовлені переважно самою природою промислового шпигунства як таємною формою конкурентної боротьби.

У сучасних умовах більшість банків-конкурентів віддають перевагу збиранню інформації про конкурентів легальними методами, використовуючи офіційні джерела: відвідування банків, аналіз відкритих матеріалів про їхню діяльність, установлення необхідних взаємовідносин із банківськими установами і міжбанківськими організаціями, клієнтами банків, укладення угод і договорів, участь у конференціях та інших форумах, де обговорюються проблеми діяльності банків.

Запитання для самоперевірки:

1. Дайте визначення поняттю «промислове шпигунство».
2. Що є метою і об’єктом здійснення промислового шпигунства?

Питання 4. Заходи банку щодо організації захисту від промислового шпигунства

При вивченні даного питання слід запам’ятати, що *основними формами захисту банківської діяльності від промислового шпигунства є:*

1. Постійний аналіз інформації, що подається про банк у ЗМІ.
2. Контроль інформації, яка надається банком для оприлюднення.
3. Створення системи категоріювання інформації за ступенями обмеження доступу до неї.
4. Створення у банку відповідної нормативної бази з питань захисту його інформації.
5. Розосередження важливої інформації за різними її носіями.
6. Застосування технічних, програмних та криптографічних засобів захисту інформації.
7. Правовий захист інтелектуальної власності банку.
8. Проведення заходів протидії промисловому шпигунству в роботі з персоналом банку.
9. Встановлення особливого режиму функціонування інформації з обмеженим доступом банку.
10. Створення надійної системи збереження інформації.
11. Створення і забезпечення ефективної роботи системи спеціального діловодства.

Забезпечення постійного контролю за станом, режимом доступу і функціонуванням інформаційних ресурсів банку.

Запитання для самоперевірки:

1. Назвіть основні заходи банку щодо захисту від промислового шпигунства.
2. Які з перерахованих заходів є найбільш ефективними? Чому?

Тема 4. Інформаційна безпека фінансових і банківських установ

Питання для обговорення:

1. Технічні заходи і можливості вилучення інформації.
2. Фактори, що створюють загрози витоку (передання) інформації.
3. Право банків на комерційну таємницю і його юридичне закріплення.
4. Конфіденційна інформація банку, її статус та зміст.
5. Відповідальність за незаконний збір і розголошення відомостей, що становлять банківську і комерційну таємницю.
6. Заходи банку щодо попередження, виявлення та локалізації випадків протиправних посягань на банківську і комерційну таємницю, конфіденційну інформацію.

Методичні рекомендації:

Питання 1. Технічні заходи і можливості вилучення інформації

Вивчаючи дане питання, варто звернути увагу на те, що способи отримання інформації можуть використовуватись конкурентами, промисловими шпигунами, спецслужбами за допомогою створення так званих каналів витоку та передавання інформації.

Такими каналами є: візуально-оптичні (спостереження, відео-, фотозйомка), акустичні та акустоперероблювальні, електромагнітні (в тому числі й магнітні та електричні), матеріально-речові (магнітні носії, папір, фотографії тощо).

Візуально-оптичні канали створюються як оптичний шлях від об'єкта інформації до її отримувача. Для цього необхідні енергетичні, часові та просторові умови і відповідні технічні засоби. Особлива цінність інформації, отриманої через такий канал, полягає в тому, що вона є максимально достовірною, оперативною і може бути документальним підтвердженням отриманих відомостей.

Джерелом створення акустичного каналу є тіла та механізми, які здійснюють вібрацію або коливання, наприклад голосові зв'язки людини, елементи машин, що рухаються, телефонні апарати, звукопідсилювальні системи, гучномовні засоби, засоби звукозапису та звуковідновлення та ін.

Матеріально-речові канали отримання інформації створюються через вивчення відходів виробничої діяльності (зіпсовані документи або їх фрагменти, чернетки різних поміток, записів, листів тощо), викрадення, несанкціоноване ознайомлення, копіювання, фотографування, відеозапис документів, креслень, планів, зразків технічних або програмних засобів.

Запитання для самоперевірки:

1. Які існують канали витоку та передачі інформації?
2. Яким чином вони функціонують?

Питання 2. Фактори, що створюють загрози витоку (передання) інформації

При вивченні даного питання слід зазначити, що до факторів, які створюють умови витоку (передання) інформації, за дослідженнями спецслужб, відносять такі:

- надмірна балакучість співробітників банків;
- прагнення працівників банків заробляти гроші будь-яким способом і будь-якою ціною;
- відсутність у банку системи заходів, спрямованих на захист інформації;
- звичка співробітників банків ділитись один з одним почутими новинами, чутками, інформацією;
- безконтрольне використання інформаційних систем;

– наявність передумов для виникнення серед співробітників конфліктних ситуацій.

Запитання для самоконтролю:

1. Назвіть фактори, що створюють загрози витоку інформації.
2. Які з них є найбільш небезпечними?

Питання 3. Право банків на комерційну таємницю і його юридичне закріплення

Слід звернути увагу на те, що згідно зі ст. 60 Закону України «Про банки і банківську діяльність» до банківської таємниці належить інформація про діяльність і фінансовий стан клієнта, що стала відома банку у процесі його обслуговування і взаємовідносин із ним або з третіми особами під час надання послуг банком, розголошення якої може завдати матеріальної чи моральної шкоди.

Тлумачення поняття комерційної таємниці дається у ст. 30 Закону України «Про підприємства в Україні». Зокрема у статті вказується, що під комерційною таємницею підприємства розуміють відомості, пов'язані з виробництвом, технологічною інформацією, управлінням фінансами та іншою діяльністю підприємства, що не є державною таємницею, розголошення (передання, витік) яких може завдати шкоди його інтересам.

Поняття «конфіденційної інформації» наведено в Законі України «Про інформацію», де зазначено, що така інформація за своїм правовим режимом є інформацією з обмеженим доступом і її становлять «… відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов» (ст. 30).

Правовий режим доступу до банківської таємниці встановлено Законом України «Про банки і банківську діяльність». Згідно зі ст. 62 цього Закону інформація, що становить банківську таємницю фізичних осіб - клієнтів банку, розкривається банком на письмовий запит або з письмового дозволу власника інформації, а також на письмову вимогу або за рішенням суду.

Запитання для самоконтролю:

1. Дайте визначення поняття «банківська таємниця»?
2. Дайте визначення поняття «комерційна таємниця»?
3. Якими документами закріплюється право банків на конфіденційну інформацію, банківську таємницю та комерційну таємницю?

Питання 4. Конфіденційна інформація банку, її статус та зміст

При вивченні даного питання слід звернути увагу на те, що відповідно до ч. 3 ст. 30 Закону України «Про інформацію» власникам конфіденційної інформації надано право самим включати її до категорії конфіденційної, визначати режим доступу до неї і встановлювати систему (способи) її захисту.

Окремо визначено правовий режим захисту інформації, яка міститься в автоматизованих системах, що для банків є особливо необхідним, оскільки

понад 65 % банківської інформації міститься якраз в автоматизованих системах. Законодавством установлено, що доступ до інформації, яка зберігається, обробляється і передається в автоматизованих системах, здійснюється згідно з правилами розмежування доступу, які встановлюються власником інформації чи уповноваженою ним особою (ст. 6 Закону України «Про захист інформації в автоматизованих системах»). Тобто і в цьому разі право захисту інформації покладено на її власника - банк.

Запитання для самоперевірки:

1. Дайте визначення поняття «конфіденційна інформація»?
2. Які існують способи захисту конфіденційної інформації?

Питання 5. Відповідальність за незаконний збір і розголошення відомостей, що становлять банківську і комерційну таємницю

Опрацьовуючи дане питання, студентам потрібно звернути увагу на те, що відповідно до чинного законодавства за посягання на комерційну та банківську таємниці може наставати кримінальна, цивільна, адміністративна або дисциплінарна відповідальність.

Кримінальна відповідальність може настати за дії, передбачені ст. 231 «Незаконне збирання з метою використання або використання відомостей, що становлять комерційну таємницю» і ст. 232 «Розголошення комерційної таємниці» Кримінального кодексу України.

Під незаконним збиранням з метою використання відомостей, що становлять комерційну таємницю, розуміють умисні дії, спрямовані на отримання відомостей, що становлять комерційну таємницю, з метою розголошення чи іншого використання цих відомостей (комерційне шпигунство), а також незаконне використання таких відомостей, якщо це спричинило істотну шкоду суб'єкту господарської діяльності. Такі дії караються штрафом від 200 до 1000 неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до п'яти років, або позбавленням волі на строк до трьох років.

Запитання для самоперевірки:

1. Що розуміють під незаконним збиранням відомостей, що становлять комерційну таємницю?
2. Яка відповідальність чекає за незаконний збір і розголошення відомостей, що становлять банківську і комерційну таємницю?

Питання 6. Заходи банку щодо попередження, виявлення та локалізації випадків протиправних посягань на банківську і комерційну таємницю, конфіденційну інформацію

Потрібно усвідомити, що для вирішення зазначених питань банку насамперед необхідно юридично закріпити правовий статус його комерційної таємниці. Такий статус оформлюється шляхом визначення і внесення відповідних положень до документів, що регламентують діяльність банку.

Вітчизняними банками напрацьовано деякий досвід організації захисту їхньої інформації з обмеженим доступом. Організація захисту ґрунтується на нормативній базі банків, яка регламентує це питання. Насамперед відповідні положення про захист комерційної таємниці включаються до Статуту банку. Зокрема, в них вказується право банку на:

- комерційну таємницю;
- самостійне визначення складу й обсягу відомостей, що становлять комерційну таємницю і конфіденційну інформацію банку;
- захист комерційної таємниці.

Такі положення, зафіксовані в статуті, дають банку юридичне право організовувати захист його таємниць; включати вимоги щодо захисту комерційної таємниці в усі договори й угоди комерційного характеру; домагатися відшкодування збитків, завданих від посягання на інформацію з обмеженим доступом; видавати нормативні та інші документи з питань захисту банківської і комерційної таємниці; створювати відповідні підрозділи захисту таємниць банку.

Запитання для самоперевірки:

1. На чому ґрунтується організація захисту інформації з обмеженим доступом?
2. Що саме забезпечують положення про захист інформації з обмеженим доступом?

Розділ 2. Підходи до забезпечення фінансово-економічної безпеки фінансових і банківських установ

Тема 5. Фінансово-економічна безпека фінансових і банківських установ

Питання для обговорення:

1. Сутність, зміст і обумовленість фінансово-економічної безпеки фінансових і банківських установ.
2. Безпека банківських операцій.
3. Заходи безпеки під час проведення валютних операцій.
4. Забезпечення безпеки роботи банків із пластиковими платіжними засобами.
5. Заходи безпеки під час проведення розрахункових та касових операцій.

Методичні рекомендації:

Питання 1. Сутність, зміст і обумовленість фінансово-економічної безпеки фінансових і банківських установ

Слід звернути увагу на те, що *економічна безпека банку* - це стан, за якого забезпечується економічний розвиток і стабільність діяльності банку, гарантований захист його фінансових і матеріальних ресурсів, здатність адекватно і без суттєвих втрат реагувати на зміни внутрішньої і зовнішньої ситуації.

Сутність економічної безпеки банку реалізується в системі критеріїв і показників. Критерієм економічної безпеки є оцінка економічного стану банку з точки зору найважливіших процесів, які відображають сутність економічної безпеки. Критеріальна оцінка економічної безпеки базується на оцінках: ресурсного потенціалу банку і можливостей його розвитку; рівня ефективності використання ресурсів; рівня можливостей банку протистояти загрозам його економічній безпеці та самостійно ліквідовувати їх; конкурентоспроможності банку; цілісності та масштабів структури банку; ефективності кадрової політики банку.

У системі показників економічної безпеки доцільно виділити: темпи зростання прибутковості та посилення економічної стабільності; рівень матеріального і соціального забезпечення працівників банку; розмір боргових зобов’язань банку; структуру дебіторської заборгованості; використання тіньового капіталу та ін. Для економічної безпеки велике значення мають не стільки самі показники, скільки їх порогове значення, тобто допустимі величини, недотримання яких перешкоджатиме нормальному розвиткові діяльності банку, призводитиме до формування негативних тенденцій в його економічній безпеці. Найвищий ступінь економічної безпеки банку досягається за умови, що весь комплекс показників перебуває в межах допустимих

порогових значень, а порогове значення одного показника досягається не за рахунок іншого.

Запитання для самоперевірки:

1. Дайте визначення поняття «економічна безпека».
2. Назвіть основні критерії економічної безпеки.

Питання 2. Безпека банківських операцій

При вивченні даного питання варто звернути увагу на те, що у всій сукупності банківських операцій чи не найголовніше місце посідають кредитні операції. Як показує практика банківської діяльності, значну частку доходів банки отримують саме від кредитних операцій. Разом з тим якраз на тлі кредитної діяльності банки зазнають особливо великих збитків, а в деяких випадках кредитна діяльність банків і зовсім стає фатальною для них.

Досвід показує, що якоїсь єдиної системи заходів безпеки кредитних операцій, яка була б притаманна всім банкам, в Україні не існує. Банки, використовуючи існуючу законодавчу і нормативну базу, виробляють свої заходи і з тією чи іншою ефективністю застосовують їх для захисту своєї кредитної діяльності.

Слід звернути увагу, що комерційним банкам надається право самостійно аналізувати, вивчати діяльність потенційних позичальників, визначати їх кредитоспроможність, прогнозувати ризик неповернення кредиту і приймати рішення про надання або відмову у наданні кредиту.

Як правило, заходи безпеки класифікуються за терміном розвитку кредитних взаємовідносин банків з їхніми клієнтами: підготовка до надання кредиту та його надання, кредитний моніторинг у ході кредитних операцій і робота щодо повернення кредитів. Особливо слід наголосити, що забезпечення безпеки кредитних операцій не є прерогативою чи завданням якогось одного підрозділу банку (наприклад, підрозділу безпеки), заходи безпеки реалізуються всіма підрозділами, залученими у таких операціях.

Запитання для самоконтролю:

1. Чи існує єдина система заходів безпеки банківських операцій? Поясніть.
2. Яким чином класифікуються заходи безпеки банківських операцій?
3. Хто забезпечує безпеку банківських операцій?

Питання 3. Заходи безпеки під час проведення валютних операцій

Література: 25; 26**.**

Слід запам’ятати, що серед операцій банків значне місце посідають валютні операції. Тому захист таких операцій, особливо операцій, пов’язаних з міжнародними розрахунками, має також важливе значення в системі економічної безпеки банків.

Однією з найбільш значущих сфер валютного й експортного контролю є операції за міжнародними торговельними розрахунками.

Найбільш поширеною формою міжнародних розрахунків за експортно-імпортними операціями в нашій країні є акредитивна форма, при застосуванні якої необхідно керуватися «Уніфікованими правилами і звичаями для документарних акредитивів», розробленими і затвердженими Міжнародною торговельною палатою.

Для оплати імпортних товарів за допомогою акредитива, покупець звертається до банку з заявою про відкриття акредитива, заява надається банку в двох примірниках. Ця заява повинна фактично повторювати всі відповідні умови контракту. Оскільки відкриття акредитива передбачає зобов'язання банку здійснити платіж проти документів, що відповідають умовам контракту, банк повинен ретельно проаналізувати подану заяву.

Аналіз проводиться шляхом послідовного розгляду кожного пункту заяви.

У разі позитивного розгляду заяви і прийняття рішення щодо відкриття акредитива банк виконує відповідні дії, передбачені технологією таких операцій. Наступним важливим з точки зору безпеки моментом є розгляд наданих експортером документів та прийняття рішення за ними. Тут слід чітко керуватись принципом суворої відповідності тексту наданих документів умовам акредитива (банк може здійснити платіж тільки проти тих документів, які повністю відповідають акредитиву) та строків відвантаження товарів і надання документів (банк має право не здійснювати платежі за документами, які надані пізніше певної дати та терміну). Слід зауважити, якщо в акредитиві не вказана дата надання документів, то вона збігається з датою закінчення строку дії акредитива. При цьому термін між датою відвантаження та датою надання документів не повинен перевищувати 21 день, якщо в акредитиві не передбачено інше.

У термін, що не перевищує семи робочих днів, банк зобов'язаний ретельно перевірити документи, надані бенефіціаром.

Запитання для самоперевірки:

1. Чим пояснюється важливість забезпечення безпеки операцій за міжнародними торговельними розрахунками?
2. Яким чином здійснюється акредитивна форма розрахунків за експортно-імпортними операціями?
3. Як забезпечуються заходи безпеки під час проведення валютних операцій?

Питання 4. Забезпечення безпеки роботи банків із пластиковими платіжними засобами

При вивченні даного питання варто звернути увагу на те, що Останнім часом значного поширення набувають операції банків з пластиковими платіжними картками. Разом з тим, простежується тенденція до зростання втрат банків, які здійснюють такий вид діяльності, через шахрайство з пластиковими платіжними картками. Тому банки вимушені звертати значну увагу на забезпечення безпеки цих операцій. На сьогодні банківські установи вже мають відповідний досвід щодо забезпечення безпеки таких операцій, який у цілому

ґрунтується на комплексному підході організації їх захисту протягом усіх циклів, з яких ці операції складаються. Зокрема, такий підхід включає:

– розроблення і вдосконалення нормативної бази технологій як самих платіжних карток, так і операцій з ними;

– протидію втратам банків від шахрайських дій у процесі емісії та еквайрингу;

– навчання співробітників банку та підприємств торгівлі (послуг) і складання ними кваліфікаційних іспитів на допуск до роботи з банківськими продуктами - платіжними картками.

Запитання для самоперевірки:

1. Яким чином забезпечується безпека роботи банків із пластиковими картками?
2. Які документи створюють базу для формування нормативних документів з безпеки операцій з платіжними картками?

Питання 5. Заходи безпеки під час проведення розрахункових та касових операцій

Слід звернути увагу на те, що важливе місце у забезпеченні економічної безпеки банків має безпека касових операцій. Насамперед це пов’язано з тим, що якраз такі операції здійснюються безпосередньо з готівкою, посягання на яку мають найбільш активний та агресивний характер. Більше того, такі посягання, як правило, здійснюються відкрито та зухвало, з наявністю загрози життю, здоров’ю працівників банків та їхніх клієнтів. Тому цим операціям банки приділяють особливу увагу з погляду безпеки їх проведення.

Забезпечення безпеки касових операцій здійснюється в двох напрямках: особливим обладнанням приміщень банків, де проводяться такі операції, та робочих місць працівників банків, зайнятих у них; особливою поведінкою працівників банків під час емісійно-касової роботи. У першому випадку згідно з будівельними нормами банківських споруд приміщення касових сховищ, прибуткових, вечірніх та видаткових кас, інші приміщення касових вузлів, підходи (під’їзди) до них обладнуються необхідними засобами застереження, захисту, сповіщення і підлягають ретельній охороні.

Особлива поведінка працівників касових вузлів визначається відповідними нормативними актами, зокрема Інструкцією з організації емісійно-касової роботи в установах банків України (№ 1) затвердженою Постановою Правління НБУ № 129 7 липня 1994 р. зі змінами і доповненнями в редакції Постанови Правління НБУ № 309 від 1 травня 2001 р. та іншими документами нормативно-правового характеру.

Слід урахувати, що особлива увага приділяється забезпеченню безпеки проведення прибутково-видаткових операцій. Такі операції здійснюються протягом операційного дня банку. Для приймання готівки після завершення операційного дня в банках організовуються вечірні каси, режим роботи яких визначається керівниками банківських установ.

Запитання для самоперевірки:

1. Чим пояснюється важливість забезпечення забезпеки касових операцій?

2. Яким чином забезпечується безпека проведення касових і розрахункових операцій?

Тема 6. Інформаційно-аналітичне забезпечення банку

Питання для обговорення:

1. Визначення об’єктів і джерел інформації.
2. Аналіз ділової обстановки. Збір інформації.
3. Інформаційний моніторинг у банку.
4. Мета та завдання аналітичної роботи, її програмне та технічне забезпечення, алгоритм роботи з інформацією.
5. Стратегічна і тактична інформація.

Методичні рекомендації:

Питання 1. Визначення об’єктів і джерел інформації

При вивченні даного питання варто звернути увагу на те, що під ***інформаційним ресурсом*** комерційної фірми, банку розуміють сукупність юридичної, фінансової, ділової, технічної, технологічної та іншої інформації, яка перебуває в розпорядженні фірми, банку і використовується ними для забезпечення виробництва, проведення комерційних операцій, надання послуг, а також для управління їх діяльністю.

В основі формування інформаційних ресурсів лежать методи збору інформації, характерні для розвідувальної діяльності. Тому заходи інформаційно-аналітичного забезпечення діяльності банку насамперед будуть ґрунтуватись на засадах комерційної розвідки.

Об’єктами комерційної розвідки є передусім конкуруючі структури, підприємства, організації, які надають подібні послуги, виробляють аналогічні товари або у той чи інший спосіб впливають чи можуть впливати на діяльність даного підприємства, банку і в яких зосереджена або виробляється необхідна даному підприємству, банку інформація. В окремих випадках об’єктами комерційної розвідки також можуть бути технології виробництва товарів або послуг, комерційні операції.

Безпосереднє отримання інформації може здійснюватись через відповідні носії (джерела) такої інформації. Джерелами необхідної для комерційної розвідки інформації можуть бути люди (працівники відповідних установ, організацій, підприємств, банків, приватні детективи, інші категорії громадян, які з тих чи інших причин мають доступ до відповідної інформації), документи, засоби масової інформації, рекламні продукти, матеріали наукових досліджень, виробничі зразки, електронні носії інформації.

Запитання для самоконтролю:

1. Дайте визначення поняття «інформаційні ресурси банку».

2. Дайте визначення поняття «комерційна розвідка».
3. Назвіть основні об’єкти комерційної розвідки.
4. Назвіть основні джерела комерційної розвідки.

Питання 2. Аналіз ділової обстановки. Збір інформації

Варто запам’ятати, що за існуючих в Україні умов розвідувальна діяльність комерційних підприємств, банків зосереджується в основному навколо інформаційно-аналітичної роботи і забезпечується шляхом збору інформації з відкритих джерел та її аналітичного дослідження.

Структура інформаційно-аналітичної роботи (ІАР) має всі ознаки структури комерційної розвідки і передбачає організацію роботи, збір інформації та її обробку. У свою чергу, організація ІАР включає:

- визначення сфер та об’єктів інформаційної уваги підприємства, банку;
- визначення мети і завдань ІАР;
- підбір (підготовку) сил і засобів для проведення заходів ІАР;
- планування роботи;
- визначення і постановку завдань виконавцям;
- забезпечення заходів ІАР;
- контроль діяльності сил і засобів, залучених до виконання завдань ІАР.

Збір інформації передбачає вжиття таких заходів:

- створення інформаційних каналів;
- вибір об’єктів інформації, визначення і придбання (отримання) її джерел;
- організація роботи з інформаційними джерелами, отримання (споживання) інформації;
- забезпечення безперервної роботи джерел інформації.

Запитання для самоперевірки:

1. Що включає організація інформаційно-аналітичної роботи?
2. Назвіть основні заходи, що здійснюються при зборі інформації.

Питання 3. Інформаційний моніторинг у банку

При вивченні даного питання необхідно запам’ятати, що під час *інформаційного моніторингу* проводиться контроль отримання підрозділами й установами банку інформації, появи нової інформації в інформаційному середовищі банку, визначається її цінність і важливість для формування інформаційних ресурсів та забезпечення його безпеки. У ході моніторингу здійснюються: оцінка інформації та її розподіл за інформаційними базами даних, виявлення неправдивої або шкідливої інформації та визначення джерел надходження такої інформації, формування інформаційних потоків залежно від завдань, які вирішує банк. У процесі інформаційного моніторингу забезпечується своєчасна реакція на зміни в інформаційних каналах та пошук додаткових джерел інформації.

Запитання для самоперевірки:

1. Дайте визначення поняття «інформаційний моніторинг».
2. Яким чином проводиться інформаційний моніторинг?

Питання 4. Мета та завдання аналітичної роботи, її програмне та технічне забезпечення, алгоритм роботи з інформацією

Вивчаючи це питання, в першу чергу необхідно зрозуміти, що банки, проводячи інформаційно-аналітичну роботу, виробили відповідну структуру її органів. В узагальненому вигляді така структура передбачає інформаційно-аналітичний підрозділ сил безпеки банку та посади економістів-аналітиків у підрозділах його установ. Основними завданнями інформаційно-аналітичного підрозділу є:

- участь у формуванні інформаційних ресурсів банку;
- створення інтегрованих інформаційних баз даних;
- інформаційно-аналітичне дослідження об'єктів сфери інформаційної уваги банків;
- організація та проведення інформаційного аудиту й інформаційного моніторингу;
- розроблення інформаційних документів для забезпечення управлінських рішень керівництва банку;
- інформаційно-аналітичне дослідження клієнтів, партнерів, конкурентів та інформаційно-аналітичне забезпечення операцій і угод банку.

Інформаційно-аналітична робота з дослідження конкретного об'єкта включає три повністю самостійні аспекти, в кожному з яких необхідно розглянути наявні факти.

Перший аспект - *вивчення існуючого становища*. Для розгляду питань у цьому аспекті необхідно мати тільки так звані «голі» факти, які підбираються у такий спосіб, щоб вони вказували на відповідні закономірності та тенденції існування (діяльності) об'єкта, який досліджується.

Другий аспект - *вивчення можливостей*, тобто потенціалу об'єкта, причому як можливостей загальних — без протидії об'єкту, так і можливостей за умов активної протидії його розвитку. Тут слід звернути увагу на те, наскільки ефективно можуть бути реалізовані такі можливості об'єкта за конкретних умов, скажімо, притаманних відповідним банківським операціям.

Третій аспект - *вивчення (визначення) намірів об'єкта*, його можливих дій за тих чи інших умов. Тут насамперед аналізуються сприятливі та несприятливі фактори для дій об'єкта, порівнюється становище і поведінка даного об'єкта з іншими об'єктами, визначаються верхні та нижні межі розвитку (дій) об'єкта, його уразливі місця.

Запитання для самоперевірки:

1. Назвіть основні завдання інформаційно-аналітичного підрозділу банку.
2. Що включає інформаційно-аналітична робота з дослідження конкретного об'єкта?

Питання 5. Стратегічна і тактична інформація

При вивченні даного питання, необхідно усвідомити, що інформаційні системи мають дворівневу ієрархічну структуру і складаються з підсистеми стратегічної та прогнозної інформації та системи тактичної та оперативної інформації.

Слід розрізняти поняття централізованого та децентралізованого підходів до координації діяльності підсистем обох рівнів:

І рівень - підсистема стратегічної та прогнозної інформації, яка використовує текстову та кількісну інформацію, що надходить з усіх доступних банку джерел, у тому числі від консультантів, експертів і фірм, що професійно займаються збиранням, обробкою та продажем спеціалізованої інформації.

ІІ рівень - підсистема тактичної та оперативної інформації, що використовує дані аналізу фінансової діяльності банку, а також інформацію, отриману під час контактів співробітників з колегами на конференціях тощо.

У процесі гармонізації діяльності цих двох рівнів виникають досить великі проблеми, пов'язані з можливостями отримання «непрофільної», зайвої й навіть шкідливої інформації різними користувачами.

Запитання для самоперевірки:

1. Поясніть структуру інформаційної системи.
2. Поясніть значення та зміст стратегічної та прогнозної інформації.
3. Поясніть значення та зміст тактичної та оперативної інформації.

Тема 7. Організація безпеки в роботі з персоналом банку

Питання для обговорення:

1. Заходи безпеки під час прийняття працівників на роботу в банк.
2. Правила перевірки кандидатів.
3. Робота з кандидатами у період терміну випробовування.
4. Контроль роботи персоналу, ознаки можливих негативних дій працівників банку.
5. Конфлікти та їх негативний вплив на стан безпеки банку, попередження та вирішення конфліктів.

Методичні рекомендації:

Питання 1. Заходи безпеки під час прийняття працівників на роботу в банк

Вивчаючи це питання, в першу чергу необхідно зрозуміти, що важливою складовою забезпечення безпеки в роботі з персоналом банку є відповідна його кадрова політика, яка б, з одного боку, сприяла, мінімізації загроз від персоналу банку, а з іншого - стимулювала б прагнення кожного з працівників до ефективної роботи. В основу такої політики має бути покладена мінімально ризикована система комплектування банку кадрами.

Насамперед, заміщення вакантних посад повинно відбуватися тільки на конкурсних засадах, банк завжди повинен мати вибір фахівців, а не комплектувати посади за вимушеним принципом, погоджуючись на пропозиції будь-кого з претендентів. Конкурсні засади головним чином передбачають такі процедури: підбір, перевірку, оцінку, відбір, розстановку кадрів.

Як правило, інформація, отримана в результаті вивчення кандидата, не буває остаточною для прийняття рішення про зарахування його на роботу, оскільки вона лише дає змогу зробити висновок про характер і професійні якості кандидата. Але для прогнозування майбутньої поведінки тільки таких даних ще не досить. Тому значне місце у підборі кандидатів відводиться психологічному тестуванню.

Запитання для самоперевірки:

1. Якою має бути кадрова політика банку?
2. Які процедури передбачаються конкурсними засадами заміщення вакантних посад?

Питання 2. Правила перевірки кандидатів

Варто запам'ятати, що сформувавши на підставі загальних критеріїв списки кандидатів, банк перевіряє їх за двома напрямками: визначення професійної придатності фахівця для роботи в банку та виявлення його психологічної схильності до такої роботи. Крім того, однією з причин перевірки є визначення ознак, які б указували на наявність у кандидата шкідливих для роботи в банку рис (азарт, залежність від наркотичних речовин або алкоголю, порочні звички, нездорова заздрість, загострене почуття помсти тощо).

Перевірка професійних здібностей кандидатів здійснюється, як правило, фахівцями того підрозділу банку, до якого планується направити того чи іншого кандидата, та фахівцями кадрового підрозділу. У ході перевірки вивчаються подані кандидатами документи, характеристики та рекомендації на них, проводяться бесіди, а також необхідні випробування. Останні можуть здійснюватись за допомогою відповідних тестів, виконання практичних завдань, контролю поведінки в спеціально створених ігрових ситуаціях.

Запитання для самоперевірки:

1. За якими критеріями банк перевіряє кандидатів на заміщення вакантної посади?
2. Хто здійснює перевірку професійних здібностей кандидатів?

Питання 3. Робота з кандидатами у період терміну випробовування

При вивченні даного питання варто звернути увагу на те, що у деяких випадках може виникати необхідність додаткової підготовки прийнятих на роботу в банк працівників, особливо на посади, пов'язані з виконанням нових видів робіт, освоєнням нових технологій тощо. У таких випадках робота працівника в банку може розпочинатися з його короткострокового навчання.

Велике значення для формування банківського фахівця, скорішого оволодіння ним своїми обов'язками має правильна організація становлення

працівників банку на посаді. Цей період роботи фахівця, як правило, охоплює три етапи: ознайомлювальний, організаційний, адаптаційний. Під час першого етапу, яким керує безпосередній керівник підрозділу, куди призначено працівника, останній ознайомлюється з основними підрозділами банку, їх розташуванням, особливостями і завданнями свого підрозділу, характером його діяльності, посадовими обов'язками працівника і відповідальністю за їх виконання. Тут же новий працівник знайомиться з колективом підрозділу, де він працюватиме. Перший етап виконується протягом першого дня роботи.

На цьому етапі з працівником проводяться відповідні інструктажі, у тому числі і з заходів безпеки, він також мусить взяти відповідні зобов'язання щодо дотримання у таємниці і не розголошення інформації банку з обмеженим доступом.

Запитання для самоперевірки:

1. З яких етапів складається період становлення працівників банку на посаді?
2. Чим характеризується перший етап становлення працівників банку на посаді?

Питання 4. Контроль роботи персоналу, ознаки можливих негативних дій працівників банку

Вивчаючи це питання, в першу чергу необхідно зрозуміти, що контроль роботи працівників банку проводиться з метою виявлення об'єктивного стану справ щодо якості, ефективності виконання ними виробничих завдань і своїх службових обов'язків, сумлінності та творчості фахівців на своїх робочих місцях, ознак можливого виникнення негативних ситуацій та загроз діяльності банку. Серед заходів контролю можуть застосовуватись різні види перевірок, опитування думки колег, отримання відгуків, вивчення поведінки працівників у колективі і на своїх робочих місцях, періодичне тестування, звіти тощо.

Запитання для самоперевірки:

1. З якою метою проводиться контроль роботи працівників банку?
2. Які заходи контролю можуть застосовуватись до працівників банку?

Питання 5. Конфлікти та їх негативний вплив на стан безпеки банку, попередження та вирішення конфліктів

Варто запам'ятати, що конфлікт - це зіткнення протилежних інтересів, думок, оцінок окремих людей або груп людей у процесі їх спільної діяльності чи виконання однієї (близької за змістом) роботи.

Конфлікти в банку можуть бути внутрішніми (між окремими працівниками, групами працівників одного колективу) і зовнішніми - між колективами підрозділів одного банку та колективами банків. Небезпечними для банку є всі конфлікти, але найбільш тяжкі наслідки можуть бути в результаті внутрішніх конфліктів. Як правило, вони відбуваються дуже емоційно і хворобливо, бувають тривалими, їх характер набуває антагоністичних.

Розглядаючи ті чи інші конфліктні ситуації, керівникові необхідно бути максимально об’єктивним, не підтримувати жодної сторони. Спокійно вислухати кожну з них і спробувати розібратися в ситуації, подивившись на неї з однієї та з другої позиції. У разі необхідності треба порадитись з фахівцями, психологами, працівниками кадрових органів. Можна обговорити ситуацію на зборах колективу, хоча це може бути не завжди виправданим. Якщо виявлено порушення кадрової дисципліни, моральних норм, трудових угод, необхідно вжити всіх заходів до виправлення ситуації і задовольнити всі обґрунтовані претензії. Один із виняткових заходів - заміна керівника колективу або його тимчасове усунення (направлення на навчання, у відрядження тощо).

Щоб запобігти виникненню конфліктів, необхідно правильно формувати колектив. У кожної людини свій рівень сприйняття, темперамент, почуття, які залежно від віку, освіти, фаху можуть розвиватись різними темпами, за різними напрямками. У колективі такі властивості особистості працівників виражаються через сприйняття й оцінки (людини, діяльності, проблеми і т. д.).

У результаті цього виникають різні позиції і погляди відносно одного й того самого об’єкта. За певної відсутності однотипних властивостей характерів членів колективу такі погляди і позиції можуть бути приводом для конфліктів. Тому, формуючи колектив, поряд з професійними вимогами до співробітників необхідно приділяти увагу і їхнім психологічним особливостям, які б забезпечували психологічну сумісність.

Запитання для самоперевірки:

1. Дайте визначення поняття «конфлікт».
2. Які існують види конфліктів?
3. Назвіть заходи запобігання конфліктам.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Нормативні документи:

1. Закон України «Про банки і банківську діяльність». Відомості Верховної Ради України. 1991. № 11.
2. Закон України «Про захист інформації в автоматизованих системах». Відомості Верховної Ради України. 1994. № 31. Ст. 286.
3. Постанова НБУ «Про затвердження Положення про порядок здійснення банками операцій з векселями в національній валюті на території України» від 16.12.2002 р., №508. URL : http://zakon.nau.ua/doc/?code=z0174-03.
4. Інструкція про порядок регулювання діяльності банків України. Постанова Правління НБУ від 28.08.2001р., № 368. URL : http://zakonl.rada.gov.ua.

Основна:

1. Зубок М..Г. Безпека банківської діяльності : навчально- методичний посібник для самостійного вивчення дисципліни. К.: КНЕУ. 2003. 156 с.

2. Орлюк О.П. Банківська система України. Правові засади організації. К. : Юрінком Інтер, 2003. 376 с.

3. Ніколалюк С.І., Никифорчук Д.Й. Безпека суб'єктів підприємницької діяльності : курс лекцій. К. : КНТ, 2005. 320 с.

4. Побережний С.М., Пластун О.Л., Болгар Т.М. Фінансова безпека банківської діяльності : навчальний посібник для самостійного вивчення дисципліни «Безпека банків». Суми : ДВНЗ «УАБС НБУ», 2010. 112 с.

Додаткова:

1. Адаменко С.І. Характеристика та класифікація загроз у банківській системі України. *Стратегічна панорама*. 2004. № 4. С. 48-52.

2. Барановський О.І. Банківська безпека : проблема виміру. *Економіка і прогнозування*. 2006. № 1. С. 7-26.

3. Болгар Т.М. Менеджмент ризиків і ресурсів як складова забезпечення фінансової безпеки банківських установ. *Вісник Львівської комерційної академії*. Серія економічна. Вип. 27. Львівська комерційна академія. Львів, 2007. С. 37-41.

4. Фінансова безпека підприємств і банківських установ : монографія / За заг. редакцією док-ра екон. наук., проф. А.О. Єпіфанова, [А.О.Єпіфанов, О.Л. Пластун, В.С.Домбровський та ін.]. Суми : ДВНЗ «УАБС НБУ», 2009. 295 с.

Інформаційні ресурси

1. Украинский банковский портал. URL : http://banker.ua/officialrating/?gclid=CN3Q6Iz0i7UCFcVY3godKXcArA (дата звернення : 01.09.2019).

2. Путеводитель для банкиров. URL : http://www.prostobankir.com.ua/spravochniki/reytingi_bankov (дата звернення : 01.09.2019).