МІЖРЕГІОНАЛЬНА
АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ

МАУП

ПРОГРАМА
вивчення дисципліни

“БАНКІВСЬКА БЕЗПЕКА”

Київ 2000

Підготовлено кандидатом економічних наук, доцентом
В. Є. Бондаренком

Затверджено на засіданні кафедри банківської та страхової справи (Протокол № 6 від 15.03.2000)

Схвалено Вченою радою Міжрегіональної Академії управління персоналом

Бондаренко В. Є. Програма вивчення дисципліни "Банківська безпека". — К.: МАУП, 2000. — 15 с.

Методична розробка містить пояснювальну записку, навчально-тематичний план, програмний матеріал до вивчення дисципліни "Банківська безпека", теми практичних і лабораторних занять, вказівки до курсового проектування, а також список рекомендованої літератури.

ПОЯСНЮВАЛЬНА ЗАПИСКА

Пов'язаний зі значними прибутками всесвітній банківський бізнес породжує гостру конкуренцію між окремими банкірами, які у боротьбі за клієнта не тільки намагаються прискорити та поліпшити обслуговування, пропонують нові, зручніші умови і послуги, а й за допомогою комерційної розвідки вдаються до усіх легальних і нелегальних засобів, щоб виявити можливі напрямки діяльності, стратегічні задуми конкурентів.

До того ж, великий капітал завжди перебуває під пильним наглядом злочинних угруповань, які активно шукають шляхів, аби зібрати щедрий нетрудовий ужинок на чужій ниві. Статистика свідчить, що лише внаслідок проникнення злодіїв до банківських комп'ютерних систем банки втрачають від 143 млн до 41 млрд дол. на рік.

Отже, проблема банківської безпеки стає дедалі актуальнішою. Адже сучасні інформаційні технології, що базуються на комп'ютерних мережах, дозволяють злодіям і зловмисникам, не виходячи із власного помешкання, псувати інформацію, грабувати банки й комерційні структури, розташовані не тільки в іншій країні, а й на іншому континенті.

НАВЧАЛЬНО-ТЕМАТИЧНИЙ ПЛАН
вивчення дисципліни
“БАНКІВСЬКА БЕЗПЕКА”

№ п/п	Назва теми
1	Основні поняття і методи сучасної комерційної розвідки
2	Організаційні та технічні засоби безпечної роботи банку
3	Правові основи безпеки банку
4	Технічні та програмні засоби інформаційної технології і проблеми їх захисту
5	Типові загрози безпеці фінансових систем і банківській діяльності
6	Проектування систем безпеки банку
7	Шифрування інформації
8	Соціально-психологічні аспекти порушення безпеки
9	Банківська безпека і кадрова політика
10	Особиста безпека і дії в екстремальних ситуаціях
11	Протидія комерційних банків бандитсько-терористичним діям

ПРОГРАМНИЙ МАТЕРІАЛ
до вивчення дисципліни
“БАНКІВСЬКА БЕЗПЕКА”

Тема 1. Основні поняття і методи сучасної комерційної розвідки

Суть розвідки полягає в організації та проведенні заходів, спрямованих на збирання необхідної інформації, її обробку й одержання висновків про можливості та задуми як окремих осіб, так і фірм у цілому. Економічна розвідка має три аспекти: організація розвідки, здобування інформації та її обробка. Метою розвідки у галузі комерційної діяльності є усунення факторів, шкідливих для діяльності банку, та сприяння його ефективному розвитку.

Одержання інформації здійснюється через такі носії: люди, документи, технічні засоби (підслуховування, нагляд тощо), виробничі зразки. Тому у розвідці працюють з трьома компонентами — людиною, технікою, інформацією.

У розвідці існують свої правила, методики, закони, секрети.

Підрозділ фірми, який реалізує завдання розвідки і охорони, називається службою безпеки (аналітична служба, інформаційна служба та ін.). Служба безпеки налічує від 2–3 до 5–10 осіб. Як правило, це оперативні

працівники, аналітики, практики-маркетологи, спеціалісти з технічних засобів, криптографи, психологи, соціологи, журналісти, юристи.

Тема висвітлює методи роботи комерційної розвідки, а також технічні засоби підтримки її роботи.

Тема 2. Організаційні та технічні засоби безпечної роботи банку

Безпека банку організується за такими основними напрямками: фізичний, технічний та інтелектуальний захист банку і його технологій, правовий захист, робота з внутрішнім і зовнішнім середовищем, наукові дослідження в галузі безпеки.

Голова правління і керівник служби безпеки банку (СББ) визначають основні напрямки організації безпеки. Після цього у процесі проектування системи безпеки, очолюваного керівником СББ,
окреслюються мета і завдання СББ, знаходяться співвідношення між різними видами безпеки: фізичним, технічним, інтелектуальним, правовим. Формулюються положення, що регламентують діяльність банку з питань безпеки, і виходячи з них встановлюється режим роботи банку. Опрацьовуються питання безпеки в кадровій політиці, методи організації охорони та розмежування доступу до різних приміщень банку, технічні засоби забезпечення такого розмежування.

Тема розкриває технологію проектування системи захисту банку.

Тема 3. Правові основи безпеки банку

Робота підрозділів економічної розвідки часто може перебувати на межі діяльності, окресленої законодавчими актами. Так, відповідно до ст. 148(6–7) КК України збирання відомостей, що становлять комерційну таємницю, карається позбавленням волі на 2–3 роки. Тому банківському персоналу необхідно знати законодавство, основні поняття якого наведені далі.

Конфіденційна інформація — інформація, яка є власністю осіб (фізичних, юридичних) і розповсюджується за їх бажанням (відповідно до ст. 30 Закону України “Про інформацію”).

Комерційна таємниця — відомості, які не є державною таємницею, але розповсюдження яких може завдати шкоди підприємству (відповідно до ст. 30 Закону України “Про підприємства”).

Банківська таємниця — відомості про операції, рахунки та вклади клієнтів і кореспондентів.

Тема висвітлює законодавчі акти, що регламентують діяльність служби безпеки в нашій країні.

Крім того, наводяться відомості про зарубіжні законодавчі акти.

Тема 4. Технічні та програмні засоби інформаційної технології та проблеми їх захисту

Сучасні інформаційні технології базуються на комп'ютерних методах обробки даних і широко використовують комп'ютерні мережі для обміну фінансовою інформацією. З погляду безпеки такі мережі є найвразливішим елементом, який потребує особливої уваги. Тим більш, що преса постійно повідомляє про спроби проникнути до комп'ютерної мережі задля фінансових вигод або просто задля забави. Здебільшого йдеться про обчислювальні мережі великих корпорацій. Але якщо локальні обчислювальні мережі (ЛОМ) банку підключені до національних або міжнародних інформаційних комунікаційних систем, вони так само стають об'єктами "проникнень".

Грабіжник або вандал може підключитись до мережі в одній з численних точок, закритих від звичайного нагляду або просто увійти до системи зі зручного персонального комп'ютера і вкрасти або зіпсувати дані. На жаль, чим легше користуватися системою, тим більше можливостей для незаконних користувачів.

Тому захист інформації в ЛОМ набув великого значення, і багато які продавці обчислювальної техніки постачають системи захисту ЛОМ.

У темі розглядаються методи захисту окремих комп'ютерів від програм-вірусів, які вводяться зловмисниками для псування інформації; шляхи захисту як локальних, так і глобальних обчислювальних мереж: персональна ідентифікація, паролі, а також організаційні заходи; введення програмного "контрольного журналу", який наглядає за системою паролів. Крім того, даються основні відомості про виробників і постачальників комп'ютерної техніки.

Тема 5. Типові загрози безпеці фінансових систем і банківській діяльності

Правоохоронні органи (СБУ, ФБР та ін.), викриваючи комп'ютерні злочини, нагромадили значний досвід і багату картотеку типових методів, які використовують злодії для проникнення до комп'ютерних систем банків.

На основі цього досвіду в темі розкрито класифікацію загроз. Наводяться відомості про основні злочинницькі методи атакування банківських систем: “салямі”, “закриті канали”, “маскарад”, “збір сміття”, “люки”, “троянський кінь”, віруси та ін.

Розглядається захист від підробки пластикових карток. Аналізуються порушення використання пластикових карток, загрози при розрахунках у точці продажу (“зворотне трасування”, “пряме трасування”).

Тема 6. Проектування систем безпеки банку

Перш ніж оцінити кількість грошей і часу, що вкладаються у захист даних, необхідно кількісно визначити ступінь ризику втрати даних, тому проектування системи захисту починається з аналізу ризику. Предметом вивчення є деякі елементи аналізу ступеня ризику, які допоможуть отримати уявлення про цінність даних, що захищаються, та можливості їх втрати.

Далі наводиться класифікація можливих каналів втрат інформації і на основі певної моделі захисту проектується система безпеки. Тема аналізує кілька моделей захисту.

Найдостовірнішими та такими, що відповідають дійсності, можна вважати ігрові моделі захисту, тобто моделі, в яких є мінімум дві сторони. Гра починається зі створення першою стороною певної системи захисту. Після цього друга сторона починає долати цю систему, а перша — будує нову. Якщо друга сторона подолала захист до того, як було створено новий, перша сторона програла. Якщо ж на момент подолання захисту вона має нову систему захисту, то вона виграє. Незалежно від результату першого раунду гра триває. Критерієм ефективності системи захисту в цьому підході є функція двох аргументів — часу, витраченого на створення системи захисту, та часу, витраченого на її подолання. Можна розглядати і складніші ігрові моделі, які враховують не тільки час, а й вартість захищуваної інформації та витрати на розробку/подолання системи захисту.

Розробка системи захисту має здійснюватися разом із розробкою системи, яку належить захищати. Досвід створення систем захисту дозволяє виділити основні принципи, яких необхідно дотримуватись під час проектування. Тема досить повно розкриває ці принципи.

Оцінювання системи безпеки виконується на основі видань Національного центру комп’ютерної безпеки (NCSC): “Критерій оцінки безпеки

комп'ютерних систем" (оранжева книга) та "Керівництво по застосуванню оцінки безпеки комп'ютерних систем у специфічних оточеннях" (жовта книга). Класи захисту: Д, С1, С2, В, В1, В2, В3, А1. Процес сертифікації триває від 0,5 до 3 років.

Тема 7. Шифрування інформації

Захист даних за допомогою шифрування — одне з можливих рішень проблеми їх безпеки. Зашифровані дані стають доступними тільки для того, хто знає, як їх розшифрувати, і тому викрадення зашифрованих даних є абсолютно безглуздим для несанкціонованих споживачів.

У темі розглядаються найбільш ефективні стандарти в області криптозахисту інформації: DES (Data Encryption System) — стандарт шифрування даних, який широко використовується для захисту інформації, зокрема банківської; RSA (Rivest, Shamir, Adleman) — криптосистема з відкритими ключами (частина ключа відома всім); MAA (Message Authentication Algorithm) — розроблений в Англії стандарт для захисту фінансових повідомлень; MAC (Message Authentication Code) — код перевірки вірогідності даних.

У Росії Федеральним агентством урядового зв'язку та інформації (ФАПСИ) запроваджено з 1990 р. стандарт криптографічного перетворювання ГОСТ 28147–89, для якого характерна дуже висока криптостійкість — 10^{75}.

Тема 8. Соціально-психологічні аспекти порушення безпеки

Дослідження італійських соціологів показують, що 25 % персоналу банків абсолютно чесні люди, 25 % — зрадники, 50 % — особи, які діють згідно з обставинами. На думку експертів у нашій країні це відповідно: 10 %, 10 %, 80 %. Отже, знайти необхідного інформатора, як правило, не є нездоланною проблемою для розвідки конкурента, оскільки 90 % службовців — потенційні зрадники.

Крім того, близько 80 % усіх злочинів, що мають місце у середовищі електронних систем, скоюються або співробітниками банку, або за їхньою допомогою (дані щодо західних банків).

Виходячи з цього одним з важливих завдань СББ є створення необхідних умов, за яких працівнику було б невигідно порушувати безпеку. Необхідно виховувати фірмовий патріотизм. СББ має вести роботу зі службовцями банку, поліпшуючи психологічний клімат у колективі.

У темі розглядається японський досвід патріотичного виховання співробітників. Багато уваги приділяється мові рухів, що дозволяє працівнику служби безпеки виявляти настрій і психологічний стан співробітників та може сприяти профілактиці злочинів.

Тема 9. Банківська безпека і кадрова політика

Останнім часом практика свідчить, що переважна більшість злочинів і порушень у банку пов'язана з діями працівників банку. У зв'язку з цим доцільно з метою підвищення безпеки приділяти більше уваги підбору і вивченню кадрів банку; проводити роз'яснювально-виховну роботу, систематичні інструктажі та вивчати правила і методи безпеки. Велику увагу необхідно приділяти професійному відбору службовців.

Особливу увагу зосереджено на вивченні усіх аспектів професійного відбору службовців. Розглядаються психологічні тести, що оцінюють різні аспекти особистості (тести Айзенка, РСК, КУ-СОРТ, Томаса, УСК, Кеттела, СМИЛ та ін.).

Тема 10. Особиста безпека і дії в екстремальних ситуаціях

Специфіка роботи у банківський сфері така, що її працівники (особливо керівні) інколи мусять контактувати з правоохоронними органами і представниками кримінальних структур дещо частіше аніж представники інших професій.

Стосовно кримінальних структур це може бути шантаж, рекет, нагляд, різні види нападу, стосовно правоохоронних органів — здебільшого обшук, затримання, арешт.

У темі обговорюються проблеми стереотипу поведінки працівника комерційної структури у таких екстремальних ситуаціях.

Тема 11. Протидія комерційних банків бандитсько-терористичним діям

Аналіз оперативних даних вказує на те, що стосовно комерційних банків як національні, так і інтернаціональні злочинні угруповання все ширше застосовують жорстокі методи диверсійно-провокаційної діяльності, яка часто має характер бандитсько-терористичних актів.

У темі, підсумовуючи вітчизняний і зарубіжний досвід, розглядаються спеціальні методи впливу на працівників банків (викрадення, вбивства, психологічний терор, публікації дезінформації, підрив ділової репу-

тації), основні методи і прийоми диверсійно-терористичної діяльності (вибухи, обстріли, мінування, підпали, напади, захвати, акти вандалізму); окреслюються основні напрямки боротьби з диверсійно-терористичною загрозою (формування програм забезпечення безпеки персоналу, впровадження спеціальних методів управління і кадрової політики, охорона керівництва, нейтралізація агентурних джерел злочинних елементів).

Крім того, розглядаються методи діяльності контррозвідки банківських структур, спрямовані на збирання, нагромадження й обробку інформації про можливі диверсійно-терористичні акції.

ТЕМИ ПРАКТИЧНИХ ЗАНЯТЬ

Розробка елементів проектування захисту банку

Заняття 1. Фізичний захист банку

1. Визначити гіпотетичний чи реальний банк, який необхідно захищати, його функції, структуру підрозділів і надане банку приміщення.
2. Сформувати план банку у відповідності до [4] і встановити системи захисту, вибрані з каталогів [14].
3. Розробити кошторис використаних засобів захисту.
4. Розробити структуру і склад підрозділу безпеки банку, сформувати його штатний розпис.
5. Розробити інструкцію, що регламентує діяльність працівників банку щодо забезпечення його безпеки.
6. Розробити інструкцію, що регламентує користування службовими телефонами з метою запобігання відпливу інформації.

Заняття 2. Правові основи захисту банку

Вивчити і опрацювати основні законодавчі акти України, які стосуються забезпечення безпеки діяльності банків. Написати відповідний реферат.

Заняття 3. Інформаційний захист банку

1. Визначити і відобразити на плані комп’ютерну мережу, яка підтримує діяльність банку.

2. Вибрати як засіб розмежування доступу до інформації у комп'ютерній мережі банку програмне забезпечення NetWare.
3. Визначити інформацію, що циркулює у банку в процесі його діяльності.
4. Скласти таблицю розмежування доступу до інформації різних категорій службовців банку.
5. Розробити інструкцію про порядок оформлення доступу службовців до інформаційної системи (формування і зміна паролів та прав доступу).
6. Розробити інструкцію про порядок резервування інформації, що циркулює у банківській мережі, і тестування мережі на наявність програм, що завдають шкоди (вірусів тощо).

Заняття 4. Психологічні основи захисту банку

1. Розробити інструкцію для керівного складу банку, мета якої — забезпечити у колективі добрі взаємини і виховання службовців у дусі фірмового патріотизму, що запобігало б зрадництву і виказуванню комерційної (банківської) таємниці.
2. Розробити інструкцію для службовців відділу кадрів банку щодо методики відбору претендентів на посади у банку, яка б запобігала прийому на роботу потенційно небезпечних осіб.
3. Розробити інструкцію з особистої безпеки для службовців банку.

ТЕМИ ЛАБОРАТОРНИХ РОБІТ

Робота 1. Дослідження комп'ютерних антивірусних засобів

Мета роботи. Вивчити поліфаги DRWEB і AIDSTEST і навчитися користуватися ними.

Робота 2. Дослідження стандартів шифрування інформації DES

Мета роботи. Вивчити програми шифрування інформації за стандартом DES і навчитися користуватися ними.

Робота 3. Дослідження стандарту шифрування інформації RSA

Мета роботи. Вивчити програми шифрування інформації і виконання електронного підпису за стандартом RSA і навчитися користуватися ними.

Робота 4. Дослідження програм, вилучених ФБР, що слугували засобом підбору номерів кредитних карток, які використовували злодії для оплати послуг і товарів по мережі INTERNET

Мета роботи. Вивчити програми. Виробити навички проведення аналізу.

Робота 5. Дослідження психологічних тестів Айзенка, РСК, КУ-СОРТ, Томаса, УСК, Кеттела, СМИЛ

Мета роботи. Вивчити системи психологічного тестування і опанувати навички роботи з ними.

ВКАЗІВКИ ДО КУРСОВОГО ПРОЕКТУВАННЯ

Розробка проекту захисту банку

Проект має складатися з чотирьох розділів.

1. Фізичний захист банку:

а) визначити гіпотетичний чи реальний банк, який необхідно захищати, його функції, структуру підрозділів і надане банку приміщення;

б) сформувати план банку відповідно до [4] і встановити системи захисту, вибрані з каталогів [14];

в) розробити кошторис використаних засобів захисту;

г) розробити структуру і склад підрозділу безпеки, сформувати його штатний розпис;

д) розробити інструкцію, що регламентує діяльність працівників банку щодо забезпечення його безпеки;

е) розробити інструкцію, що регламентує користування службовими телефонами з метою запобігання відпливу інформації.

2. Правові основи захисту банку:

а) опрацювати основні законодавчі акти України, що стосуються забезпечення безпеки діяльності банків;

б) написати відповідний реферат.

3. Інформаційний захист банку:

а) визначити і відобразити на плані комп'ютерну мережу банку, яка підтримує його діяльність;

б) вибрати як засіб розмежування доступу до інформації у комп'ютерній мережі банку програмне забезпечення NetWare;

в) визначити інформацію, що циркулює в банку у процесі його діяльності;

г) скласти таблицю розмежування доступу до інформації різних категорій службовців банку;

д) розробити інструкцію про порядок оформлення доступу службовців до інформаційної системи (формування і зміна паролів і прав доступу);

е) розробити інструкцію про порядок резервування інформації, що циркулює у банківській мережі, і тестування мережі на наявність програм, що завдають шкоди (вірусів тощо).

4. Психологічні основи захисту банку:

а) розробити інструкцію для керівного складу, мета якої — забезпечити у колективі добрі взаємини і виховання у службовців фірмового патріотизму, що запобігало б зрадництву і виказуванню комерційної (банківської) таємниці;

б) розробити інструкцію для службовців відділу кадрів щодо методики відбору претендентів на посади у банку, яка б запобігала прийому на роботу потенційно небезпечних осіб;

в) розробити інструкцію з особистої безпеки для службовців банку.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. *Автоматизация* расчетных операций банков и фондовых бирж. — М.: Церих-ПЭЛ, 1992. — 214 с.
2. *Банковская* система SFTBANK. Документация фирмы “40.5”. — Одесса, 1995. — 20 с.
3. *Безруков Н. Н.* Компьютерная вирусология. — К.: УРЕ, 1991. — 123 с.
4. *Відомчі* будівельні норми України. Проектування банків і банківських сховищ. ВБН В.2.2–00032106–1–95. НБУ. — К., 1995. — 41 с.
5. *Гайкович В., Першин А.* Безопасность электронных банковских систем. — М.: Единая Европа, 1994. — 345 с.
6. *Гостюшин А.* Энциклопедия экстремальных ситуаций. — М.: Зеркало, 1994. — 251 с.
7. *Давыдов И.* Тайна фирмы. — М., 1993. — 320 с.
8. *Добрович А. Б.* Воспитателю о психологии и психогигиене общения. — М.: Просвещение, 1987. — 207 с.

9. *Защита* информации в персональных ЭВМ / А. В. Спесивцев и др. — М.: Радио и Связь, 1992. — 192 с.
10. *Защита* и “раздевание” программ в MS DOS. — К., 1992. — 102 с.
11. *Казакевич Ю., Кочетов Н.* Предприниматель в опасности: способы защиты. — М.: Бизнес, 1993. — 170 с.
12. *Карнеги Д.* Как вырабатывать уверенность в себе и влиять на людей, выступая публично. — Ульяновск: Ульяновская правда, 1989. — 78 с.
13. *Касперский Е. В.* Вирусы и борьба с ними. — М., 1991. — 146 с.
14. *Каталог* фирмы РЕНАР. — К., 1998. — 48 с.
15. *Кримінальний* кодекс України. — К.: Політвидав України, 1975. — 351 с.
16. *Ларичев В. Д.* Как уберечься от мошенничества в сфере бизнеса. — М.: Юрист, 1996. — 128 с.
17. *Липис А., Маршалл Т., Линкер Я.* Электронная система денежных расчетов. — М.: Финансы и статистика, 1988. — 234 с.
18. *Мафтик С.* Механизмы защиты в сетях ЭВМ. — М.: Мир, 1993. — 216 с.
19. *Никифоров Г., Азнакиев Г.* Защита коммерческой тайны. — К.: Юринформ, 1994. — 88 с.
20. *Оучи У.* Методы организации производства. — М.: Экономика, 1984. — 184 с.
21. *Пиз А.* Язык телодвижений. — Минск, 1995. — 416 с.
22. *Скотт Д. Г.* Конфликты и пути их преодоления. — К., 1991. — 191 с.
23. *Соловьев Е.* Коммерческая тайна и ее защита. — М.: Зеркало, 1995. — 145 с.
24. *Стрельченко Ю.* Обеспечение информационной безопасности. — К.: Юринформ, 1995. — 240 с.
25. *Хофман Л. Д.* Современные методы защиты информации. — М.: Сов. радио, 1980. — 264 с.
26. *Черкасов В. В.* Деловой риск в предпринимательской деятельности. — К.: Либра, 1996. — 153 с.
27. *Шварц М.* Сети связи. — М.: Наука, 1992. — 458 с.
28. *Ярочкин В.* Служба безопасности коммерческого предприятия. — М.: Ось-89, 1995. — 144 с.

ЗМІСТ

Відповідальний за випуск *Н. В. Медведєва*
Редактор *І. О. Денісов*
Комп’ютерна верстка *Т. Г. Замура*

Зам. № ВКЦ-472

Міжрегіональна Академія управління персоналом (МАУП)
03039 Київ-39, вул. Фрометівська, 2, МАУП