**Практичні завдання для самостійного виконання:**

1. Ви працюєте в операційному підрозділі банку, здійснюєте обслуговування рахунків працівників крупної корпорації. Ваш колега говорить, що знає всіх цих працівників і впевнений у тому, що свої рахунки вони не контролюють. Тому можна впевнено невеликими сумами списувати кошти з цих карткових рахунків на фіктивний рахунок. Але для цього ви повинні дозволити йому заходити в банківську мережу і операційний день під вашим іменем. Які ваші дії в такій ситуації? Як запобігти незаконним діям працівника?

2. Вийшовши з кабінету за викликом керівника, ви залишили свій телефон. Коли ви повернулися, то ваш колега телефонував комусь із вашого телефону. До того ж ви помітили, що ваш колега заходив з вашого комп’ютера в облікову програму банку. Проте, ніяких операцій не здійснював. Після цього випадку ви помітили, що ваш телефон прослуховується. Чи винні ви в тому, що сталося? Як ви будете протидіяти колезі? Чи можливим буде уникнення неправомірного прослуховування вашого телефонного пристрою?

3. Під час здійснення банківської операції ви помітили, що до банківської інформації здійснюється несанкціонований доступ. Ви не розумієте чим це може закінчитися для банку і для вас особисто. Які ваші дії в даній ситуації? До кого слід звернутися? І яким чином можна запобігти незаконному доступу до інформації?

**Контрольні запитання**

1. Охарактеризувати комплекс заходів щодо забезпечення безпеки електронних платежів.

2. Що таке система технічного захисту інформації банків?

3. Описати структуру системи технічного захисту інформації банків.

4. Що таке підсистема захисту від несанкціонованого доступу до інформації?

5. Дати визначення поняття “система забезпечення безпеки даних”.