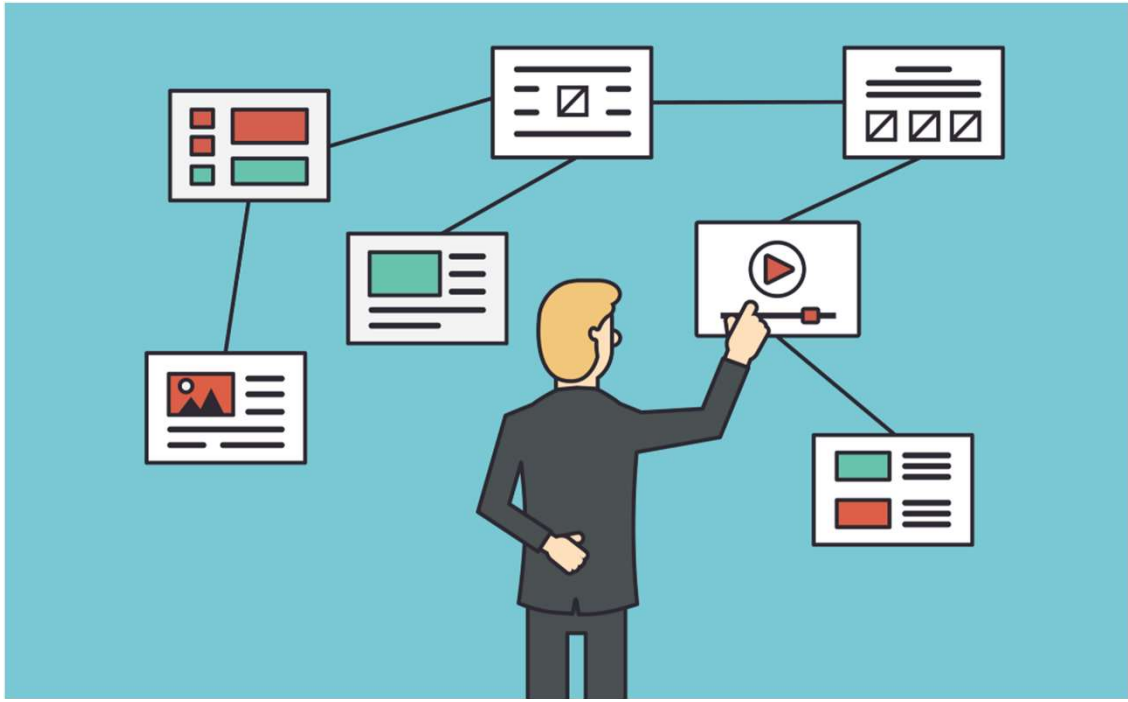
Введення в дисципліну. Правове забезпечення банківської безпеки

Лектор:
Лимаренко Вячеслав Володимирович
к.т. 066-070-8586

Структура курсу

- 10 лекцій (24 години, не оцінюються);
- 6 лабораторних робіт (24 години, 60 балів max);
- Екзамен (40 балів max).



Введення в дисципліну

Банківська діяльність пов'язана з обробкою великих обсягів інформації, основну частину яких складають конфіденційні дані клієнтів.

До них відноситься особисті дані користувачів, копії їх документів, номери рахунків, дані про проведені операції, транзакції та ін.

У процесі роботи з цією інформацією важливо, щоб вона не потрапила до рук зловмисників, не була змінена чи втрачена.

Введення в дисципліну

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.

Системою забезпечення безпеки є комплекс правових, організаційно-керівних, спеціальних, соціально-психологічних, режимних, технічних, профілактичних та пропагандистських мір, спрямованих на якісну реалізацію захисту банку від зовнішніх та внутрішніх загроз його безпеці та діяльності.

Чинники підвищення кількості загроз

– залучення в процес інформаційної взаємодії все більшого числа людей і організацій;
– підвищення рівня довіри до банківських систем управління і обробки інформації;
– ставлення до інформації, як до товару;
– концентрація великих обсягів інформації різного призначення і приналежності на електронних носіях;
– наявність інтенсивного обміну інформацією між учасниками цього процесу;
– кількісне і якісне вдосконаленням способів доступу користувачів до інформаційних ресурсів;
– диференціація рівнів втрат (збитків) від знищення, модифікації, витоку або незаконного блокування інформації;
– різноманіття видів загроз і можливих каналів несанкціонованого доступу до інформації;
– зростання числа кваліфікованих користувачів ЕОМ і можливостей по створенню ними програмно-технічних впливів на банківські системи;
– перехід до ринкових відносин, з властивою їм конкуренцією і різними видами розвідки.

Загроза інформації

Під **загрозою інформації** що обробляється в автоматизованій системі (АС) маються на увазі будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації чи нанесення збитків автоматизованій системі, тобто:

- порушення конфіденційності інформації;
- порушення цілісності інформації;
- порушення доступності інформації

Банківські дані

До банківських даних належить сукупність інформації, що забезпечує можливість подання фінансової установи в інформаційному середовищі, а також дані, що забезпечують можливість проведення фінансових операцій між клієнтом та банком, а також між кількома клієнтами, які використовують банківську установу як фінансовий посередник.

Існує два види банківської інформації – це дані, які використовуються в інформаційному середовищі з метою представлення діяльності фінансової установи для її клієнтів, а також сукупність даних клієнтів фінустанови як юридичних, так і фізичних.

Незважаючи на те, що одна інформація є відкритою, а друга закритою, обидві вони потребують надійного захисту.

Безпека відкритих даних

Безпека відкритих даних полягає в тому, що ця інформація завжди має бути достовірною та подаватися клієнтам у тому ракурсі, який вибрав для себе банк. Якщо з якихось причин ці дані будуть видозмінені або підмінені, то банк може зазнати не лише суттєвих фінансових втрат, а й удару по своєму іміджу та репутації.

Безпека закритих даних

Небезпека заволодіння **закритими даними** полягає в тому, що якщо вони потраплять до рук зловмисників, вони можуть використовувати їх з метою отримання для себе неправомірного фінансового прибутку.

Це може здійснюватися шляхом проведення неправомірних фінансових операцій або за допомогою здирництва з загрозою поширити будь-яку приховану інформацію про клієнтів банку.

Спроби доступу до таємної банківської інформації

Серед способів несанкціонованого доступу до даних банків сьогодні найчастіше зустрічаються такі:

- **Фізичний доступ та подальша крадіжка потрібної інформації**. Варіантів реалізувати цей спосіб дуже багато, починаючи з крадіжки конфіденційної інформації одним із співробітників банку, який має доступ до неї та закінчуючи ймовірністю збройного нальоту з метою отримання важливих архівів, баз даних та ін.
- **Архіви можна отримати неправомірно під час створення резервних копій**. Всім відомо, що будь-яка установа робить резервування та архівування важливих даних, щоб не втратити їх під час збою інформаційної системи чи якоїсь глобальної катастрофи. Більшість банківських установ архівують свою інформацію за допомогою стримерів, записуючи дані на стрічку, що зберігається в окремих приміщеннях. Під час процесу транспортування стрічок та їх зберігання можливе копіювання даних та розповсюдження їх поза інформаційним середовищем банку.

Спроби доступу до таємної банківської інформації

- Одним з найбільш поширених і ймовірних способів витоку інформації є **несанкціонований доступ до даних через права адміністратора інформаційної системи або за допомогою спеціальних програм**, які дозволяють обійти захист та отримати доступ до потрібної інформації. Іноді співробітники можуть робити це навіть ненавмисно, наприклад, беручи роботу додому. Як би й нічого небезпечного, але ймовірність того, що дані потраплять до рук злодія, у такому разі істотно зростає.
- Ще одним способом отримати засекречену інформацію є **поширення різноманітних програм-шпигунів, вірусів, плагінів, спеціалізованого софту**.

Види загроз банківській інформації

- 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;

Види загроз банківській інформації

- 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;

Види загроз банківській інформації

- 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 переносних 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;

Види загроз банківській інформації

- 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.

Методи захисту банківської інформації

Враховуючи перелічені загрози втрати важливих даних, мають вибиратися методи та засоби захисту банківської інформації:

- **Захист від фізичного доступу.** Більшість банків приділяють велику увагу рівню фізичної безпеки своєї інформації. Починається цей процес з того, що місця, де зберігаються інформаційні архіви та встановлюються банківські сервери, мають більш високий рівень захищеності від проникнення та можливості перебування там сторонніх фізичних осіб. Крім цього, активна робота ведеться і з підбору персоналу, який матиме доступ до конфіденційних даних банку та його клієнтів. Реалізація перелічених чинників істотно знижує ймовірність крадіжки архівів, але не виключає її повністю.
- **Створення резервних копій.** Резервування інформації та запис її в архіви – це важливий крок, щоб зберегти потрібні для себе дані. Але щоб виключити ймовірність їхнього потрапляння до рук зловмисників, цей процес має відбуватися із застосуванням систем шифрування. Використання сучасного криптографічного захисту зведе нанівець ймовірність того, що навіть вкрадена інформація буде кимось використана. На сьогодні є багато різних програмних продуктів, які забезпечують шифрування даних у момент перенесення їх до архіву. Весь процес повністю автоматизований і не несе для банку істотних витрат у фінансовому плані та потребі додаткових співробітників. Також важливо, щоб у процесі створення зашифрованого архіву використовувалися сховища, збудовані на фізичних накопичувачах, а не на віртуальних. Це гарантує ще один рівень захищеності інформації, адже віртуальне сховище легше зламати, ніж реальне.

Методи захисту банківської інформації

- **Запобігання інсайдерській інформації.** Запобігти витоку інсайдерської інформації часом буває найважче. Захистити її за допомогою різних апаратних та програмних засобів – це лише половина вирішення поставленого завдання. І тут ключову роль грає людський чинник. Саме через співробітників дуже часто відбувається втрата важливих даних, що згодом впливає на майбутню та поточну діяльність банку. Тому підбір кадрів, ефективна робота внутрішньої служби безпеки та використання системи обмеження доступу дозволить мінімізувати ризики втрати інсайдерської інформації.

Завдання системи захисту банківської інформації

- 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;
- протидія 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;
- охорона 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;
- фізична та технічна охорона 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.

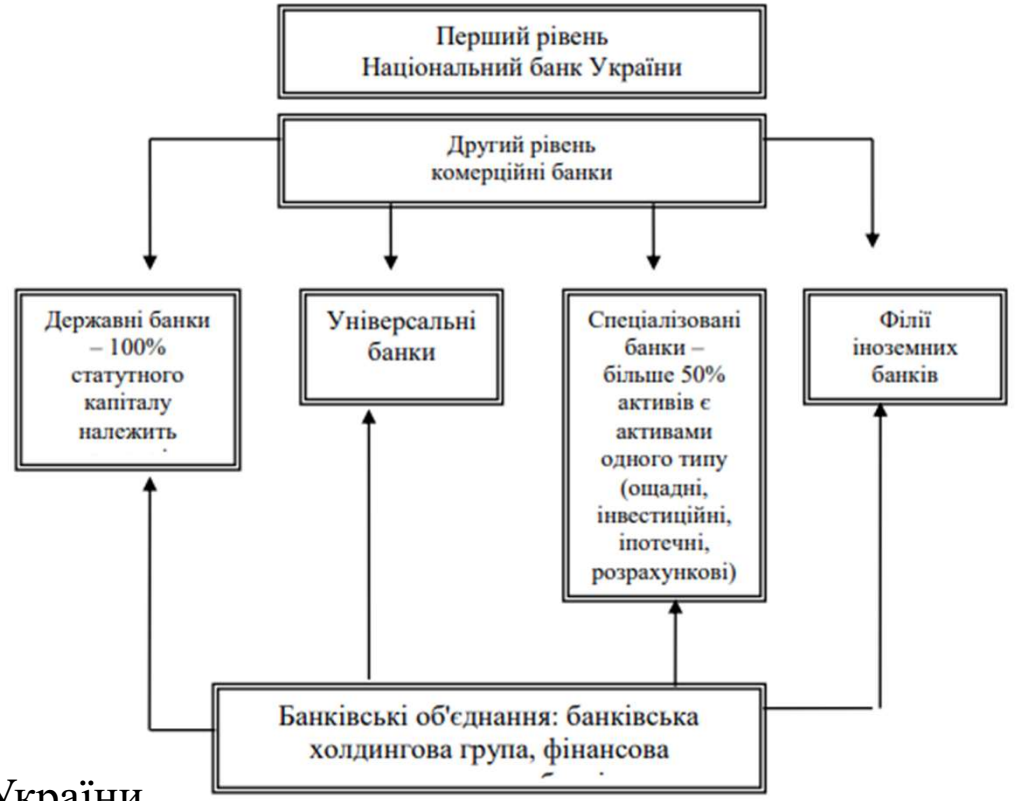
Принципи побудови системи забезпечення безпеки банку

- законність;
- поважання прав та свобод громадян;
- централізоване керування;
- координація та взаємодія з державними правоохоронними органами;
- самостійність та відповідальність;
- розумна достатність, відповідно реальним загрозам безпеки;
- застосування надсучасного матеріально-технічного оснащення;
- стимулювання суб'єктів системи;
- компетентність;
- конфіденційність;
- комплексне використання сил та засобів.

Законодавча база банківської безпеки

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

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



Структура банківської системи України

Законодавча база банківської безпеки

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

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

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

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

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

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

Законодавча база банківської безпеки

Закон України «Про Національний банк України»

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

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

Банківською таємницею, зокрема, є:

- ❑ відомості про банківські рахунки клієнтів, у тому числі кореспондентські рахунки банків у Національному банку України;
- ❑ операції, які були проведені на користь чи за дорученням клієнта, здійснені ним угоди;
- ❑ фінансово-економічний стан клієнтів;
- ❑ системи охорони банку та клієнтів;
- ❑ інформація про організаційно-правову структуру юридичної особи клієнта, її керівників, напрями діяльності;
- ❑ відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація;
- ❑ інформація щодо звітності по окремому банку, за винятком тієї, що підлягає опублікуванню;
- ❑ коди, що використовуються банками для захисту інформації.

Законодавча база банківської безпеки

Закон України «Про Національний банк України»

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

- обмеження кола осіб, що мають доступ до інформації, яка становить банківську таємницю;
- організації спеціального діловодства з документами, що містять банківську таємницю;
- застосування технічних засобів для запобігання несанкціонованому доступу до електронних та інших носіїв інформації;
- застосування застережень щодо збереження банківської таємниці та відповідальності за її розголошення у договорах і угодах між банком і клієнтом.

Законодавча база банківської безпеки

Закон України «Про платіжні системи та переказ грошей в Україні».
Розділ 8. «Захист інформації при проведенні переказу».

- Стаття 38. Вимоги щодо захисту інформації.
- Стаття 38.1. Система захисту інформації повинна забезпечувати безперервний захист інформації щодо переказу коштів на усіх етапах її формування, обробки, передачі та зберігання.
- Стаття 38.2. Електронні документи на переказ, розрахункові документи та документи за операціями із застосуванням спеціальних платіжних засобів, що містять банківську таємницю, під час їх передавання засобами телекомунікаційного зв'язку повинні бути зашифровані згідно з вимогами відповідної платіжної системи, а за їх відсутності – відповідно до законів України та нормативно-правових актів Національного банку України.
- Стаття 38.3. Порядок захисту та використання засобів захисту інформації щодо переказу визначається законами України, нормативно-правовими актами Національного банку України та правилами платіжних систем. Порядок захисту та використання засобів захисту інформації членами та учасниками міжнародних платіжних систем визначається правилами цих систем, а за відсутності в таких правилах відповідних положень – законами України та нормативно-правовими актами Національного банку України.

Законодавча база банківської безпеки

Закон України «Про платіжні системи та переказ грошей в Україні».

Розділ 8. «Захист інформації при проведенні переказу».

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

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

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

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

- Стаття 38.5. Система захисту інформації повинна забезпечувати:

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

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

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

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

Законодавча база банківської безпеки

Закон України «Про платіжні системи та переказ грошей в Україні».

Розділ 8. «Захист інформації при проведенні переказу».

- Стаття 38.6. Розробка заходів охорони, технологічних та програмно-апаратних засобів криптографічного захисту здійснюється платіжною організацією відповідної платіжної системи, її членами або іншою установою на їх замовлення.
- Стаття 39. Відповідальність суб'єктів переказу за забезпечення захисту інформації
- Стаття 39.1. Суб'єкти переказу зобов'язані виконувати встановлені законодавством України та правилами платіжних систем вимоги щодо захисту інформації, яка обробляється за допомогою цих платіжних систем. Правила платіжних систем мають передбачати відповідальність за порушення цих вимог з урахуванням вимог законодавства України.
- Стаття 39.2. При проведенні переказу його суб'єкти мають здійснювати в межах своїх повноважень захист відповідної інформації…
- Стаття 39.3. Суб'єкти переказу зобов'язані повідомляти платіжну організацію відповідної платіжної системи про випадки порушення вимог захисту інформації…
- Стаття 39.4. Працівники суб'єктів переказу повинні виконувати вимоги щодо захисту інформації при здійсненні переказів, зберігати банківську таємницю та підтримувати конфіденційність інформації, що використовується в системі захисту цієї інформації…
- Стаття 40. Порядок надання інформаційних послуг …

Законодавча база банківської безпеки

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

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

Статті Закону:

- 7 Права та обов’язки підписувачів
- 8 Центр сертифікації ключів
- 9 Акредитований центр сертифікації ключів
- 10 Засвідчувальний центр
- 11 Центральний засвідчувальний орган
- 12 Контрольний орган

Введення в дію даного закону спричинило прийняття наступних документів:

1. Постанова КМУ №903 від 13.07.2004 «Про затвердження Порядку акредитації центру сертифікації ключів»
2. Постанова КМУ №1452 від 28.10.2004 «Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності»
3. Постанова КМУ №1454 від 28.10.2004 «Про затвердження Порядку обов'язкової передачі документованої інформації»
4. Постанова КМУ №551 від 21.05.2009 «Про заходи щодо запровадження системи електронної державної реєстрації юридичних осіб та фізичних осіб – підприємців»

Законодавча база банківської безпеки

Закон «Про електронні документи та електронний документообіг».

Важливіший розділ цього Закону щодо охорони інформації є Розділ IV «Організація електронного документообігу», який складається з 5-ти статей:

стаття 14 «Організація електронного документообігу»

стаття 15 «Обіг електронних документів, що містять інформацію з обмеженим доступом»

стаття 16 «Права та обов'язки суб'єктів електронного документообігу»

стаття 17 «Вирішення суперечок між суб'єктами електронного документообігу»

стаття 19 «Відповідальність за порушення законодавства про електронні документи та електронний документообіг».

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

Законодавча база банківської безпеки

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

- ❑Стаття 162. Порушення недоторканності житла
- ❑Стаття 163. Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передається засобами зв’язку або через комп’ютер
- ❑Стаття 330. Передача або збирання відомостей, що становлять конфіденційну інформацію, яка знаходиться у володінні держави
- ❑Стаття 359. Незаконні придбання, збут або використання спеціальних технічних засобів отримання інформації
- ❑Стаття 361. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку
- ❑Стаття 361-1. Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут
- ❑Стаття 361-2. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації
- ❑Стаття 362. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї

Законодавча база банківської безпеки

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

- Стаття 363. Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється
- Стаття 200. Незаконні дії з документами на переказ, платіжними картами та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення

Законодавча база банківської безпеки

Закон «Про державну таємницю» був прийнятий 21 січня 1994 року. Цей Закон регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, її засекречуванням і охороною з метою захисту життєво важливих інтересів України у сфері оборони, економіки, зовнішніх відносин, державної безпеки й охорони правопорядку. Найбільш важливі і потрібні нам для виконання діяльності з захисту інформації та технічного захисту інформації (ТЗІ) є наступні статті Закону:

- ❑стаття 6: «Здійснення права власності на секретну інформацію та її матеріальні носії»
- ❑стаття 8: «Інформація, що може бути віднесена до державної таємниці»
- ❑стаття 10: «Порядок віднесення інформації до державної таємниці»
- ❑стаття 12: «Звід відомостей, що становлять державну таємницю»
- ❑стаття 13: «Строк дії рішення про віднесення інформації до державної таємниці»
- ❑стаття 14: «Зміна ступеня секретності інформації та скасування рішення про віднесення її до державної таємниці»
- ❑стаття 15: «Засекречування та розсекречування матеріальних носіїв інформації»
- ❑стаття 18: «Основні організаційно-правові заходи щодо охорони державної таємниці»
- ❑стаття 19: «Єдині вимоги до матеріальних носіїв секретної інформації»
- ❑стаття 37: «Контроль за забезпеченням охорони державної таємниці».

Законодавча база банківської безпеки

Закон України «Про інформацію» закріплює право громадян України на інформацію і закладає правові основи інформаційної діяльності. Нова редакція закону була прийнята Верховною Радою 9 травня 2011 року на підставі Закону Україні «Про внесення змін до закону України «Про інформацію» від 13 січня 2011 року».

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

- стаття 4: «Суб'єкти і об'єкти інформаційних відносин»
- стаття 6: п. 2 « Право на інформацію може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку, з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя»;
- стаття 10: «Види інформації за змістом»;
- стаття 11: «Інформація про фізичну особу»;
- стаття 20: «Доступ до інформації»;
- стаття 21: «Інформація з обмеженим доступом»;


Дякую за увагу
Лекцію закінчено