Аналіз чинного законодавства показує, що на регулювання відносин опіки та піклування можуть «претендувати» особистий закон (lex personalis) опікуна чи піклувальника, підопічної особи (це може бути право країни громадянства або місця проживання цих осіб); право країни, орган якої встановив опіку чи піклування; право країни, орган якої призначив опікуна чи піклувальника; право країни, де знаходиться майно, щодо якого встановлюється опіка чи піклування.

Проаналізувавши досвід колізійного регулювання опіки та піклування в іноземних країнах дійшли до висновку, що подальше вдосконалення законодавства України в цій сфері, приєднання до інших міжнародних конвенцій і договорів з міжнародного приватного права, може стати запорукою належного правового регулювання опіки та піклування, з метою забезпечення особистих немайнових і майнових прав підопічних осіб. Головним завданням сучасної юридичної науки є систематизація та узагальнення накопиченого теоретичного матеріалу та вироблення на його основі ефективних правових засобів подолання недоліків та прогалин в сфері опіки та піклування з іноземним елементом і усунення суперечностей між колізійними нормами національного та міжнародного права.

БЕРНАЗ-ЛУКАВЕЦЬКА О. М.

Національний університет «Одеська юридична академія»,
доцент кафедри цивільного права, кандидат юридичних наук, доцент

ІНФОРМАЦІЙНА БЕЗПЕКА ФІНАНСОВИХ УСТАНОВ

Під інформаційною безпекою розуміють стан захищеності інформації та інформаційного середовища від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати неприйнятного збитку суб'єктам інформаційних відносин, (в тому числі власникам і користувачам інформації). Захистом інформації є комплекс заходів, які спрямовані на забезпечення інформаційної безпеки.

Найпоширеніша модель інформаційної безпеки базується на забезпеченні трьох властивостей інформації: конфіденційність, цілісність і доступність.

Під конфіденційністю інформації потрібно розуміти те, що з нею може ознайомитися тільки обмежене коло осіб, встановлене її власником. У випадку, коли доступ до інформації отримує неуповноважена особа, відбувається її втрата.

Щодо цілісності інформації, то вона визначається її здатністю зберігатися в неспотвореному вигляді. Неправомірні, і не передбачені власником зміни інформації призводять до втрати цілісності.

Доступність інформації визначається здатністю системи надавати своєчасний безперешкодний доступ до інформації суб'єктам, що володіє відповідними повноваженнями. Знищення або блокування інформації (в результаті помилки або навмисного дії) призводить до втрати доступності, яка є важливим атрибутом функціонування інформаційних систем, орієнтованих на обслуговування клієнтів.

Крім перерахованих трьох властивостей додатково виділяють ще дві властивості, важливих для інформаційної безпеки: автентичність і апелювання. Автентичністю є можливість достовірно встановити автора повідомлення, а до апелювання відноситься можливість довести, що автором є саме ця людина і ніхто інший.

Найбільш важливі вимоги безпеки, що повинні бути реалізовані в системах електронного документообігу, наступні:

- аутентифікація та авторизація – перевірка заявленої ідентичності та надання права доступу;
- цілісність – підтримка цілісності даних і виявлення змін;
- конфіденційність – дані не можуть бути передані стороннім особам або системам;
- незаперечність – версифікатор може отримати докази, що підтверджують цілісність та походження даних;
- погодження – отримання, облік, відстеження інформованої згоди пацієнта на доступ до його медичних даних;
- аудит – всі дії повинні бути записані в хронологічному порядку;

Проблема захисту інформації у сфері банківських послуг та формування систем інформаційної безпеки на даний час є достатньою актуальною. Для того щоб її уникнути необхідно розуміти з якими загрозами можна стикнутись.

На думку І.О. Ларіної та Т.Ю. Мазуріної, до рейтингу значущості загроз відносяться: навмисне розкрадання інформації всередині організації; недбалість співробітників, що допустили витік інформації; апаратні та програмні збої; шкідливі програми; зовнішнє фінансове шахрайство; хакерські атаки; стихійні лиха та катаклізми.

Сьогодні майже не залишилося суто паперових процесів, всюди використовуються комп'ютерні технології. Безготівкові гроші, цінні папери, платіжні доручення, договори, дані клієнтів – оцифровані. Так, загрози інформаційній безпеці у банківській сфері перестали бути суто технологічними, а обернулися фінансовими, іміджевими, юридичними та іншими ризиками [1, с. 61-64].

Сьогодні вся система управління захистом інформації будується на загальновідомих постулатах. Клієнт не вибере послугу у фінансовій установі, якщо не буде впевнений у збереженні своїх грошей

та персональних даних. Тому захист інформації є обов'язковою складовою частиною банківських послуг.

Всі засоби захисту інформації можна поділити на дві групи: внутрішні, а саме запобігання загроз, що виходять з внутрішніх джерел та зовнішні, що включають запобігання загроз, що виходять ззовні.

До систем захисту інформації, що забезпечують безпеку фінансової установи відносять наступні засоби захисту: фізичні, законодавчі, організаційні, програмно-технічні. Фізичні засоби захисту засновані на створенні фізичних перешкод для зловмисника, які перегороджують йому шлях до інформації (сувора система пропуску на територію і в приміщення з апаратурою або з носіями інформації). До законодавчих засобів захисту відносяться законодавчі акти, які регламентують правила використання й обробки інформації обмеженого доступу і встановлюють кримінальну відповідальність за порушення цих правил. Під організаційним розуміється захист інформації шляхом регулювання доступу до всіх ресурсів системи (технічним засобам, система безпеки телекомунікацій та зв'язку, програмним елементам тощо) [2].

Список використаної літератури:

1. Ларина О.И., Мазурина Т.Ю. Некоторые аспекты создания информационной безопасности в банке // Деньги и кредит. – 2012. – № 7. – С. 61-64.
2. Козаченко І.П., Голубєв В.О. Загальні принципи захисту інформації в банківських автоматизованих системах / І.П. Козаченко, В.О. Голубєв // [Електронний ресурс]. – Режим доступу: http://bezpeka.com/

ГЛИНЯНА К. М.

Національний університет «Одеська юридична академія»,
доцент кафедри цивільного права, кандидат юридичних наук, доцент

ПРАВО НА ОБОВ'ЯЗКОВУ ЧАСТКУ МАЛОЛІТНІХ ТА НЕПОВНОЛІТНІХ ДІТЕЙ У ЦИВІЛЬНОМУ ПРАВІ УКРАЇНИ ТА ОКРЕМИХ ЗАРУБІЖНИХ КРАЇН

Сучасне вітчизняне спадкове законодавство надає можливість кожному громадянину вільно виявити свою волю щодо майбутньої долі належного йому майна. Будь-яка дієздатна особа має право скласти заповіт та призначити на свій розсуд спадкоємців. Об'єктивна заінтересованість суб'єктів у самостійному розпорядженні належними їм правами та майном законодавчо закріплена ст. 12 ЦК України.

Принципово важливий елемент сучасного спадкового права – право спадкоємців на обов'язкову частку спадщини – виник ще в римському