До них належать:

1) норми цивільного процесуального права;

2) цивільна процесуальна правосуб'єктність;

3) процесуальні юридичні факти.

На підставі викладеного, можна зробити висновки про те, що цивільні процесуальні відносини виникають в процесі здійснення правосуддя по цивільних справах між особами, які беруть участь у справі. Ці правовідносини виникають при наявності передумов та підстав, які передбачені законом. Тільки сукупність процесуальних прав і обов'язків, процесуальних дій по їх реалізації заінтересованих осіб та суду є змістом цивільних процесуальних правовідносин [4, с. 46].

Особливостями цивільних процесуальних правовідносин є те, що вони виникають між судом, особами, які беруть участь у справі, та іншими учасниками процесу у зв'язку з їх діяльністю по здійсненню правосуддя по цивільних справах: по справах позовного, наказного та окремого провадження.

Список використаної літератури:

1. Цивільний кодекс України прийнятий Верховною Радою України 16.01.2003 г. // Відомості Верховної Ради України, 2003. – № 28-29. – Ст. 137.
2. Луспеник Д.Д. Розгляд цивільних справ судом першої інстанції // Д.Д. Луспеник – Харків,- 2006. – Ст. 24.
3. Комаров В.В. Цивільне процесуальне право України // В.В. Комаров – Х.: Консум, 2001. – Ст. 65.
4. Чечина Н.А. Гражданские процессуальные правоотношения // Н.А. Чечина – М.: Юристъ, 1996. – Ст. 46.

ДАВИДОВА І. В.

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

КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ В КОНТЕКСТІ ВИКОРИСТАННЯ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ ПРИ ВЧИНЕННЯ ПРАВОЧИНІВ

Цивільне законодавство України (зокрема, ч.ч. 1-3 ст. 207 ЦК України) визначає умови, за яких правочин може вважатися вчиненим в письмовій формі, а саме: якщо його зміст зафіксований в одному або кількох документах, у листах, телеграмах, якими обмінялися сторони; якщо воля сторін виражена за допомогою телетайпного, електронного або іншого технічного засобу зв'язку; якщо він підписаний

його стороною (сторонами). Правочин, який вчиняє юридична особа, підписується особами, уповноваженими на це її установчими документами, довіреністю, законом або іншими актами цивільного законодавства, та скріплюється печаткою. Використання при вчиненні правочинів факсимільного відтворення підпису за допомогою засобів механічного або іншого копіювання, електронно-числового підпису або іншого аналога власноручного підпису допускається у випадках, встановлених законом, іншими актами цивільного законодавства, або за письмовою згодою сторін, у якій мають міститися зразки відповідного аналога їхніх власноручних підписів.

Отже, використання ідентифікації, як інструменту встановлення особи, залишається необхідним при здійсненні відповідних правовідносин в електронній площині. Тому існує практична необхідність існування дієвої системи, яка б чітко надавала дозвіл на вчинення певних дій, отримання інформації саме тій особі, яка має право на отримання такої інформації, або вчинення відповідних правочинів. В даному випадку неможливо обійтися без електронних засобів ідентифікації, які мають прив'язку до особи (яку треба ідентифікувати за абсолютно різними характеристиками).

Однак, не достатньо розробити та застосовувати на практиці такі електронні засоби ідентифікації, має також існувати правове закріплення їх функціонування та правовий захист, яке сьогодні в українському законодавстві не є досконалі та потребують доопрацювання та оновлення. Ці питання є особливо актуальними, зважаючи на новизну у технічному застосуванні та необхідність врегулювання процесів встановлення особи, адже це найголовніша стадія здійснення будь-якому правочину.

Наразі, законодавець увів до електронної площини електронний підпис, електронний цифровий підпис, паспорт громадянина України у формі карти з безконтактним електронним носієм (та електронним цифровим підписом), а також, нещодавно, нормативно визначений регулятором – Національним банком України Bank ID [1]. Законом України «Про електронну комерцію» [2] також було введено «підпис одноразовим ідентифікатором» та «аналог власноручного підпису».

В ст. 12 Закону України «Про електронну комерцію» зазначено, що коли відповідно до акта цивільного законодавства або за домовленістю сторін електронний правочин має бути підписаний сторонами, моментом його підписання є використання: електронного підпису або електронного цифрового підпису відповідно до Закону України «Про електронний цифровий підпис», за умови використання засобу електронного цифрового підпису усіма сторонами електронного правочину, електронного підпису одноразовим ідентифікатором, визначеним цим Законом; аналога власноручного підпису (факсимільного відтворення підпису за допомогою засобів механічного або іншого копіювання, іншого

аналога власноручного підпису) за письмовою згодою сторін, у якій мають міститися зразки відповідних аналогів власноручних підписів.

Отже, відповідно до ст. 1 Закону України «Про електронний цифровий підпис» [3] електронний підпис – це дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних; а електронний цифровий підпис – це вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача.

У такому контексті виникає необхідність більш детально розглянути поняття криптографічного захисту інформації.

Зокрема, з поступовим поширенням впливу держави на інтернет, активізувалися рухи шифропанків і кіберанархістів, які виступають за право приватної переписки, яке буде гарантовано не законами на папері, а законами математичними, на які держава впливати не зможе. Основний метод захисту інформації, запропонований зазначеними течіями – використання криптографічних засобів, тобто спеціальних алгоритмів і систем шифрування, кодування або іншого перетворення інформації, в результаті якого її зміст стає недоступним без використання ключа і зворотного перетворення (розшифровки). За допомогою подібних математичних алгоритмів дані можна зашифрувати так, що розшифровка займе тривалий час (при деяких алгоритмах – кілька тисяч років), що забезпечить безпеку, а в більшості випадків ще й анонімність в мережі [4].

У більшості країн, діяльність, яка пов'язана з криптографічним захистом інформації, підлягає правовому регулюванню. В Україні розробки в сфері криптографічного захисту інформації, також законодавчо закріплені. Зокрема, відповідно до ст. 7 Закону України «Про ліцензування певних видів господарської діяльності» [5] діяльність, пов'язана з наданням послуг в галузі криптографічного захисту інформації, ліцензується.

Визначення основних понять у сфері криптографічного захисту інформації міститься в Положенні про порядок здійснення криптографічного захисту інформації в Україні, затвердженому Указом Президента України 22 травня 1998 р. [6].

Отже, криптографічний захист – це вид захисту, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

Попри те, що чинне законодавство передбачає необхідність ліцензування розробок в сфері криптографічного захисту інформації, державі все ж таки непідконтрольна діяльність вільних розробників (тобто, фізичних осіб без статусу підприємця). Адміністративні санкції за провадження діяльності без ліцензії до таких суб'єктів також застосовані

бути не можуть, оскільки обов'язок пройти процедуру ліцензування покладається виключно на суб'єктів господарювання [4].

Таким чином, в Україні безліч аспектів використання криптографії на законодавчому рівні залишаються неврегульованими. Зокрема, відсутні норми, які регламентують участь в діяльності, пов'язаної з криптографічним захистом інформації, фізичної особи без статусу суб'єкта господарювання. Також відкритим залишається питання про можливість примусового розкриття ключів шифрування користувачами на вимогу правоохоронних органів.

Разом із тим, особи, які прагнуть захистити власний особистий простір від несанкціонованого втручання шляхом розробки і застосування криптографічних алгоритмів і систем, в Україні мають можливість це зробити.

Список використаної літератури:

1. Горкуша М. Встановлення довіри до електронного підпису в Україні. – Режим доступу : https://ilaw.net.ua/vstanovlennya-doviry-do-elektronnoho-pidpysu-v-ukrajini/
2. Про електронну комерцію : Закон України від 03.09.2015 р. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/675-19
3. Про електронний цифровий підпис : Закон України від 22.05.2003 р. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/852-15
4. Горобець О. Криптография – свобода или препятствия – Режим доступу : https://ilaw.net.ua/kryptohrafyya-svoboda-yly-prepyatstvyya/
5. Про ліцензування певних видів господарської діяльності : Закон України від 02.03.2015 р. – Режим доступу : http://zakon0.rada.gov.ua/laws/show/222-19
6. Про Положення про порядок здійснення криптографічного захисту інформації в Україні : Указ Президента України від 22.05.1998 р. № 505/98. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/505/98

ДЕРЕВНИН В. С.

Национальний университет «Одесская юридическая академия»,
доцент кафедры гражданского права, кандидат юридических наук, доцент

ЗАВЕЩАТЕЛЬНЫЙ ОТКАЗ ПО ЗАКОНОДАТЕЛЬСТВУ УКРАИНЫ И НЕКОТОРЫХ ЗАРУБЕЖНЫХ СТРАН

Статья 1237 Гражданского кодекса Украины предоставляет право завещателя на завещательный отказ (легат) [1], который предоставляет собой установленную в завещании обязанность наследников исполнить какую-либо имущественную обязанность в пользу иных лиц (отказополучателей), которые имеют право требовать исполнения этой