***ВАСИЛЕНКО МИКОЛА ДМИТРОВИЧ***

*Національний університет «Одеська юридична академія», професор кафедри кібербезпеки, доктор фізико-математичних наук, доктор юридичних наук, професор, академік Міжнародної академії інформатизації*

***НОВІКОВ В'ЯЧЕСЛАВ ПАНТЕЛІЙОВИЧ***

*Національний університет «Одеська юридична академія», доцент кафедри кібербезпеки, кандидат технічних наук, доцент*

***РАЧУК ВАЛЕРІЙ ОЛЕКСАНДРОВИЧ***

*Національний університет «Одеська юридична академія», асистент кафедри кібербезпеки*

## «ЦИФРОВЕ СУСПІЛЬСТВО» НА ТЕРЕНАХ ІНФОРМАТИЗАЦІЇ: КОНФІДЕНЦІЙНІСТЬ У ТЕХНІКО-ПРАВОВИХ ПРОЯВАХ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ

Конфіденційність стала принциповою складовою існування «цифрового суспільства», складаючи найбільш вразливу його ланку. Реально саме конфіденційність унеможливлює отримання інформації неуповноваженою особою, а цілісність інформації полягає у неможливості будь-якої її трансформації неуповноваженою особою або ж уповноваженою, але без обґрунтованої на те мети при виконанні дій щодо електронних довірчих послуг. Вимоги часу щодо електронних довірчих послуг та вимоги до посилення їх конфіденційності дозволили посилити останню і зробити її універсальною, затверджуючи такий підхід на законодавчому рівні [1]. Відзначимо, що Закон [1] так і не враховував увесь спектр питань конфіденційності та не був спрямований на вирішення пов'язаних з нею задач. З аналізу технічної та юридичної сторони реалізації багатьох питань в галузі інформаційних технологій та їх захисту відомо, що технічна сторона завжди випереджає юридичну (див. [2]). Тому таке співвідношення не є дивним. Однак законодавча складова має підтягуватися до технічних змін більш швидкими темпами і, як наслідок, прийняття зазначеного вище Закону слід вважати вельми прогресивною подією. Так, Закон [1] не тільки розширив розуміння ряду дефініцій, зокрема ввівши в нього такі поняття як відкриті та особисті (закриті) ключі, кваліфікований підпис тощо, а й увів в правовий обіг визначення нових технічних понять. Однак з юридичної сторони не можна не відмітити, що Закон [1] інтегрує в собі всі попередні здобутки у сфері застосування електронних послуг в розумінні дотримання конфіденційності. Фактично в міжнародному сенсі конфіденційність щодо інформаційної безпеки є однією з основних складових частин самої цієї безпеки. В той же час фахівцям добре відомо, що конфіденційність, цілісність та доступність виступають обов'язковими вимогами, які на законодавчому рівні (державному

рівні) мають бути строго дотримані. Нехтування або неналежним чином дотримання вимог щодо конфіденційності веде до інформаційних втрат, що загалом закономірно приводить до відповідних втрат в цілому підприємства, організації, держави. Отже, конфіденційні інформаційні дані, що циркулюють, обробляються та зберігаються в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (далі системах) повинні бути надійно захищеними. Це стосується любої інформації, тим більш конфіденційної, бо навіть відкриті інформаційні дані під час обробки в системі повинні зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення. Усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією. Модифікувати або знищувати відкриту інформацію можуть лише ідентифіковані та автентифіковані користувачі, яким надано відповідні повноваження. Спроби модифікації чи знищення відкритої інформації користувачами, які не мають на це повноважень, неідентифікованими користувачами або користувачами з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися.

Зазначимо, що під час обробки конфіденційної інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення. Доступ до конфіденційної інформації надається тільки ідентифікованим та автентифікованим користувачам. Спроби доступу до такої інформації неідентифікованих осіб або користувачів з непідтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися.

Система дозволяє користувачеві надавати можливість здійснення декількох операцій з метою досягнення убезпечення інформації, або ж надає можливість позбавлення користувача такого права. Боротьбу з функцією несанкціонованого блокування може назначити власник інформаційних даних, на свій розсуд, у разі якщо такі інформаційні дані в системі законодавством не передбачені.

Для досягнення безпеки інформації необхідно дотримуватися певних правил таким чином, щоб у системі здійснювалася обов'язкова дія, яку прийнято іменувати – реєстрація. Таким чином, ми реєструємо:

– користувачів за результатами їхньої автентифікації та ідентифікації;

– будь-які спроби несанкціонованих дій з інформаційними даними;

– фактично здійснені користувачами усі операції під час обробки інформації;

– випадки змін прав доступу користувачам (надання/позбавлення) на час обробки інформаційних даних;

– дані за результатами перевірки цілісності програмно-апаратних засобів захисту інформаційних даних.

При цьому слід пам'ятати, що можливість проведення аналізу реєстраційних даних забезпечується виключно користувачем, якого

уповноважено здійснювати управління засобами захисту інформації та контроль за захистом інформації в системі (адміністратор безпеки). Реєстрація здійснюється автоматичним способом, а реєстраційні дані захищаються від модифікації та знищення користувачами, які не мають повноважень адміністратора безпеки [3]. Реєстрація спроб несанкціонованих дій з конфіденційною інформацією про фізичну особу, яка законом віднесена до персональних даних, повинна супроводжуватися повідомленням про них адміністратора безпеки як це відбувається в країнах-членах ЄС (див. [2; 4]). Результатом таких протиправних дій користувачів, які, в першу чергу, повинні бути ідентифіковані та автентифіковані, стає порушення загальної конфіденційності. Такі особи обов'язково повинні бути позбавлені права доступу до інформації та її обробки, а це означає, що контроль за станом цілісності програмно-апаратних засобів, призначених для забезпечення захисту в системі має здійснюватися автоматизованим способом. Передачу конфіденційної інформації з однієї системи до іншої необхідно здійснювати в закодованій формі або з умовами передавання спеціальними захищеними каналами зв'язку у відповідності до вимог діючого законодавства за напрямком криптографічного та технічного захисту інформаційних даних. Прийнятий порядок підключення систем, в яких обробляються конфіденційні інформаційні дані, до глобальних мереж передачі даних визначається законодавством. У системах з конфіденційною інформацією також здійснюється контроль за цілісністю програмного забезпечення, яке використовується для обробки інформації, запобігання його несанкціонованої модифікації та ліквідація наслідків такої модифікації. При цьому одночасно контролюється цілісність програмних та технічних засобів захисту інформації. У разі порушення їх цілісності обробка в системі інформації припиняється.

Для збереження конфіденційності обов'язково здійснюються організаційні засади досягнення безпеки інформаційних даних. А саме, проводиться спеціальний захист інформації від несанкціонованих дій, у тому числі від комп'ютерних вірусів. Так, для досягнення інформаційної безпеки шляхом гарантованого захисту від комп'ютерних вірусів, а також від несанкціонованих дій необхідно забезпечувати в усіх системах відповідні спеціальні заходи, а захист інформації від спеціального впливу на засоби обробки інформації має забезпечуватися в системі у разі, якщо рішення про необхідність такого захисту прийнято власником (розпорядником) інформації умова гарантованої інформаційної безпеки від спеціального впливу на технічні та програмно-апаратні засоби захисту. Тоді в системі буде досягнуто конфіденційність тільки в тому випадку, коли розпорядник (власник) інформації прийме рішення про таку необхідність. Обов'язково слід пам'ятати про те, що юридичну відповідальність за досягнення безпеки інформації в системі несуть посадові особи (керівники, заступники, керівники підрозділів інформаційної безпеки будь-якої організації, яка володіє (є розпорядником) системи з інформацією, що необхідно захищати, шляхом створення та

правильною експлуатацією цих інформаційних систем в сукупності з програмно-апаратними та технічними засобами захисту.

Таким чином, стрімкий розвиток інформатизації, розмежовуючи матеріальну та юридичну складові, стимулює розвиток як самих зазначених систем та їх конфіденційності, постійно підвищуючи її рівень. Можна з впевненістю говорити, що в сучасних інформаційних відносинах конфіденційність визначається своєю важливістю, розкриваючись як властивість обставин правової реальності, що в логіко-мовних і технічних реаліях виводить на передові рубежі саме інформатизацію. В цьому випадку конфіденційність продовжує становити властивість актів поведінки, подій, юридичних станів тощо, зберігаючи інформацію про них як сукупності певних відомостей, що потребують бути відповідним способом захищеними.

***Список використаної літератури:***


1. Закон України «Про електронні довірчі послуги» № 2155-VIII від 05.10.2017 зі змінами, внесеними згідно із Законом № 440-IX від 14.01.2020. – Відомості Верховної Ради. – 2017. – № 45. – Ст. 400.
2. Бойко В. Д., Василенко М. Д. Кібербезпека та захист персональних даних в ЄС: проблеми цифрового суспільства / В. Д. Бойко, М. Д. Василенко // Наукові праці Національного університету «ОЮА». – Т. 23. – Одеса, 2019. – С. 34–48.
3. Постанова Кабінету Міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» № 373 від 29.03.2006 р. із змінами, внесеними згідно з наступними Постановами КМУ. – Офіційний вісник України від 12.04.2006. – № 13. – Стор. 164. – Ст. 878.
4. Бойко В. Д. Кібербезпека в ЄС та країнах-членах: генезис та проблеми її підвищення / В. Д. Бойко, М. Д. Василенко, С. В. Кухаренко // Інформаційна безпека людини, суспільства, держави – К. : СБУ, 2019. – № 3. – С. 57–69.



**Ключові слова:** інформатизація, інформація, конфіденційність, несанкціонований доступ, захист, інформаційні дані, реєстрація даних, закон.

**Ключевые слова:** информатизация, информация, конфиденциальность, несанкционированный доступ, защита, информационные данные, регистрация данных, закон.

**Key words:** informatization, information, confidentiality, unauthorized access, protection, information data, data registration, law.