УДК 004.91

П. О. ГЕТМАНЮК, Ю. В. ФОРКУН

МОДЕЛІ ОНЛАЙН-СПІЛЬНОТ ЯК ОСНОВА ВЗАЄМОДІЇ УЧАСНИКІВ КОЛАБОРАТИВНОГО ДОКУМЕНТУВАННЯ

Проведено дослідження моделей веб–ресурсів, які можуть бути використані для організації комунікативних процесів учасників веб–спільнот. Проведено аналіз поняття «електронний документ». Встановлено основні та вузьконаправлені розуміння даного поняття, які можуть бути застосовані у веб-середовищі. Було проаналізовано основні функціональні, структурні та комунікативні особливості кожного з досліджуваних типів сервісів як у їх класичному вигляді, так і з сучасними можливостями їх модернізації. Внаслідок цього аналізу, було виявлено переваги та недоліки кожного з досліджуваних типів сервісів. В залежності від контексту використання поняття «електронний документ», встановлено та проаналізовано основні тенденції та варіанти використання кожного дослідженого типу веб-сервісу для забезпечення взаємодії учасників віртуальної спільноти у процесі спільного документування за допомогою засобів веб-середовища. На основі отриманих результатів, встановлено найбільш оптимальні шляхи використання існуючих моделей сайтів для організації процесу колаборативного документування. Встановлено перспективність розвитку веб–ресурсів з поєднаними моделями у рамках однієї інформаційної системи.

Ключові слова: моделі онлайн–спільнот, колаборативне документування, електронний документ, веб–ресурс, класифікація сайтів.

Проведено исследование моделей веб–ресурсов, которые могут быть использованы для организации коммуникативных процессов учасников веб–сообществ. Проведено анализ понятия «електронній документ». Установлено основные та узкоспециализированные понимания данного понятия, которые могут быть использованы в веб-окружении. Было проанализированно основные функциональные, структурные и коммуникативные особенности каждого из исследованных типов сервисов как в их классическом виде, так и с современными возможностями их модернизации. В результате этого анализа, было установлено основные сильные и слабые стороны каждого из изучаемых типов сервисов. В зависимости от контекста использования понятия «електронный документ», установлено и проанализировано основные тенденции, а также варианты использования каждого изученного типа веб-сервиса для обеспечения взаимодействий учасников виртуального сообщества в процессе совмесного документирования с помощью средств веб-среды. На основании полученных результатов, установлено наиболее оптимальные пути использования существующих моделей сайтов для организации процесса колаборативного документирования. Установлено перспективность развития веб–ресурсов с обьединёнными моделями в рамках одной информационной системы.

Ключевые слова: модели онлайн–сообществ, колаборативное документирование, електронный документ, веб–ресурс, классификация сайтов.

This research was aimed for web resources analysis, which models may be in use for organization of communicative processes between web–communities participants. The “electronic document” formalization was analyzed. Basics and more specific senses of this concept was declared, that may be applied to the web environment. The main functional, structural and communicative features of each of the studied types of services in their classical forms and with possibilities of their modernization were analyzed. As a result of this analysis, all advantages and disadvantages of each of the service-types studied were identified. Main trends and case of uses of each analyzed type of web-service were fixed, what depends on the context of “electronic document” term usage. According to results, most effective cases in use were received for different site–models in collaborative documentation process realization. Perspectives of web–resources development was found with models combining in frames of one informational system.

Keywords: models of online communities, collaborative documentation, electronic document, web–resource, site classification.

Вступ. З розвитком інформаційних технологій, все частіше впроваджуються сервіси, які сприяють кращій автоматизації різних процесів та взаємодії між користувачами. Насамперед, у процесі розвитку технологій «Веб 2.0» виникають нові потреби щодо задоволення потреб кінцевих користувачів. Даний процес є незавершеним [1], тому постійно виникають та реалізуються нові принципи та парадигми щодо функціонування програмних засобів різних сфер направленості.

Зважаючи на це, слід зауважити, що реалізація колаборативної взаємодії між учасниками віртуальних спільнот постійно модифікується, базуючись на використанні вже існуючих основоположних понять [1–7].

Об’єкт дослідження та його технологічний аудит. Об’єктом дослідження є моделі віртуальних спільнот, які можуть бути використані у процесі колаборативного документування. Кожен вид онлайн спільноти має свої технічні особливості, які реалізують його конкретні функціональні можливості.

Поняттям та категоризацією типів віртуальних спільнот займалися такі українські науковці як Андрій Пелещишин, Юрій Сєров, Соломія Федушко [1–7]. Згідно даних досліджень, було сформульовано декілька видів класифікацій віртуальних спільнот, в залежності від конкретної площини, з якої вони можуть бути оцінені. Було виділено організаційні та комунікативні види віртуальних спільнот. Для організації комунікацій між учасниками різних віртуальних спільнот використовуються такі основні види сервісів, в залежності від технічних можливостей та цільових потреб: блоги; форуми; чати; соціальні мережі; гостьова книга.

Кожна з перерахованих форм реалізації віртуальної спільноти має свої переваги та недоліки.

Мета та задачі дослідження. Постановка завдання: виконати дослідження основоположних понять та моделей онлайн–спільнот.

Мета статті: на основі проведених досліджень виконати аналіз ефективних та менш ефективних моделей та принципів функціонування онлайн–спільнот, які можуть бути використані в організації процесу колаборативного документування.

Дослідження існуючих рішень проблеми. Перед тим, як почати досліджувати види моделей сайтів, слід визначитися, які інформаційні ресурси можуть бути класифіковані під поняттям «електронний документ». Даним питанням займалися ряд вчених: І. Л. Бачило, А. П. Вершинін, В. В. Годін, Г. З. Залаев, М. І. Костомаров, М. В. Ларін, Л. В. Ткачев [8–14]. Кожен учений має свої визначення, щодо поняття електронного документу, проте в загальному розумінні – це зафіксовані інформаційні дані, які можуть бути ідентифіковані та зберігаються у цифровому вигляді.

Учені І. К. Корнєєв та В. В. Годін ствердують, що електронним документом можна вважати повідомлення в інформаційній системі, яке має усі завірені реквізити, згідно встановлених вимог [9].

Також, Г. З. Залаєв пропонує категоризацію різних видів електронних документів, в залежності від їх утворення [10]: отримані внаслідок конверсії документів, які існують матеріально у паперовій або технотронній формах; існують суто в цифровому середовищі; не базуються на паперових технологіях. Це повідомлення, які можуть пересилатися за допомогою каналів телекомунікаційного зв'язку.

Науковець І. Л. Бачило також формулює свої визначення даного поняття, серед яких є деякі спільні з попередніми авторами тези, де також присутні кілька нових понять [11]. Згідно даної праці, електронний документ може бути: як засіб інформування користувача (наприклад дисплей, або файл); як вираження волі учасника в електронній формі правовідносин.

Згідно проаналізованих тверджень, можна зробити висновок, що визначення електронного документу може відрізнятись, в залежності від контексту застосування даного поняття.

Для організації колаборативних процесів у веб–середовищі використовуються онлайн спільноти.

Слід одразу зазначити, що сервіси типу «гостьова книга» є застарілими та відносяться до комплексу технологій «Веб 1.0». Онлайн–ресурси даного типу не мають чітких комунікативних інструментів, оскільки користувачі веб–простору є простими гостями, а права редагування контенту належить лише власникам сайту [1, 2].

Чати – це окремий вид комунікації, для якого характерні відсутність зберігання історії, відсутність тематичних розділів, а також обов'язковість перебування усіх його учасників у онлайн–режимі [1]. Здебільшого, чати у «чистому» вигляді трапляються доволі рідко. Такі системи часто можуть бути інтегровані у інші веб–ресурси, для поліпшення організації комунікативних можливостей.

Більш функціонально розвинутими та поширеними на сьогоднішній момент часу є сайти типу «блог». Даною тематикою також займалися ряд вчених [1, 4].

Форуми являють собою окрему парадигму побудови веб–ресурсів для організації онлайн–спільнот. У даному випадку присутня ієрархічна система розподілу тематичних розділів на вкладені підрозділи, а також самі обговорення. Також присутня чітка класифікація користувачів, які мають конкретні фіксовані права, з можливістю їх обмеження або розширення з боку адміністраторів або модераторів сайту [5, 6].

Доволі специфічним явищем є соціальні мережі. Згідно праць вказаних вчених, можна виявити відкриті, напів–відкриті та закриті соціальні мережі [1, 2] Таким чином, закриті соціальні мережі не дозволяють побачити звичайним Інтернет–користувачам (гостям) те, що відбувається всередині них, відкриті – дозволяють, а напів–відкриті дозволяють, в залежності від виставлених налаштувань доступу.

Справа у тому, що кожна соціальна мережа має свої технічні та функціональні особливості, цільову аудиторію. Тому, використання тієї чи іншої інформаційної системи даного типу напряму зумовлене конкретними потребами її користувачів.

Результати досліджень основних типів онлайн-спільнот. В епоху розвитку технологій «Веб 2.0», важливим фактором є формування інформаційного наповнення онлайн–ресурсів учасниками віртуальних спільнот, а не лише власниками сайтів [1]. Згідно вище описаним фундаментальним категоріям популярних реалізацій веб–спільнот, користувачі кожної з них мають різні види прав та привілегій [1, 3, 5]: адміністратори; модератори; користувачі; гості.

Блоги мають дещо іншу парадигму роботи. Детально та комплексно парадигму функціонування блогу в умовах конкуренції та інших важливих чинників було досліджено С. Федушко та Ю. Сєровим [4].

Користувачі, які мають повноваження робити пости на сайти типу «блог», мають можливість генерувати будь–який текстовий матеріал, на основі власних даних та встановлених правил самого сайту. Також, автор публікації може прикріплювати власні файли текстового формату, або робити посилання на веб–ресурси, на яких вони зберігаються, звісно, якщо це дозволено адміністрацією сайту (рис. 1).

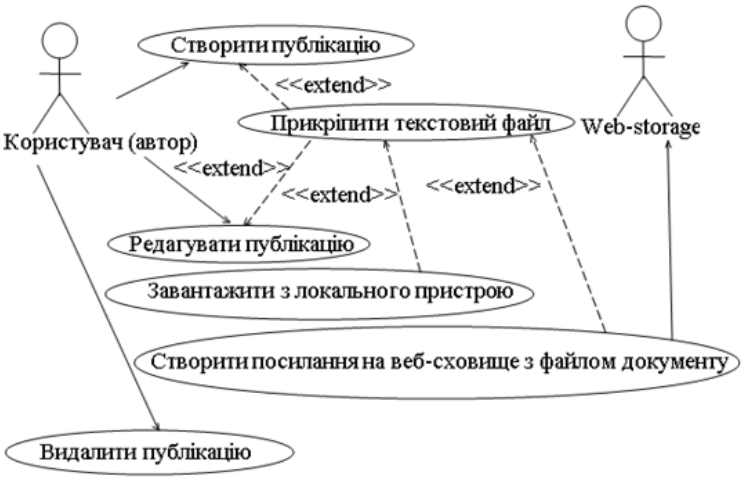

Рис. 1 – Діаграма варіантів використання розміщення файлу в публікації

У випадку, якщо користувач зробив пост, який відповідає критеріям визначення документу – такий пост також можливо вважати електронним документом [8–14]. Даний випадок вказує на фактичне розміщення повного контенту документу за конкретною адресою у веб–середовищі. Таким чином, інші користувачі матимуть змогу перенести його в інакшу форму, не змінюючи оригінал: роздрукувати на матеріальний носій інформації; скопіювати та зберегти у цифровій формі в іншому вигляді; використати засоби веб–комунікації для поширення ресурсу за допомогою посилань, або повідомлень.

Загальні активності користувача при опрацюванні контенту документа з публікації блогу наведено на діаграмі (рис. 2).

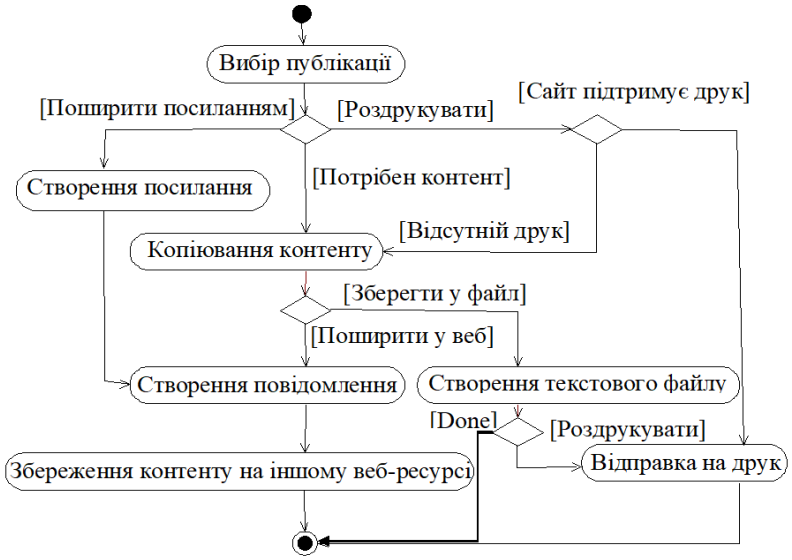

Рис. 2 – Діаграма загальних можливостей перетворення користувачем документу, представленим у якості публікації блогу

До комунікативної взаємодії учасників веб–блогу відносяться дописи, або коментарі, які інші користувачі мають змогу залишати під публікацією автора. На відміну від чатів, усі коментарі та публікації залишаються постійно. Їх видалення може бути викликане видаленням публікації, або видаленням коментаря його автором чи адміністратором сайту.

У деяких блогів існують вкладені коментарі. Їх принцип полягає у тому, що до конкретного коментаря користувачі пишуть інші коментарі, з метою дати відповідь, або підтримати тему, яку розпочав конкретний користувач своїм основоположним коментарем. Сукупність даних засобів можна відобразити у вигляді структурованого дерева з вузлами, яке формується самими користувачами під основною публікацією автора (приклад на рис. 3).

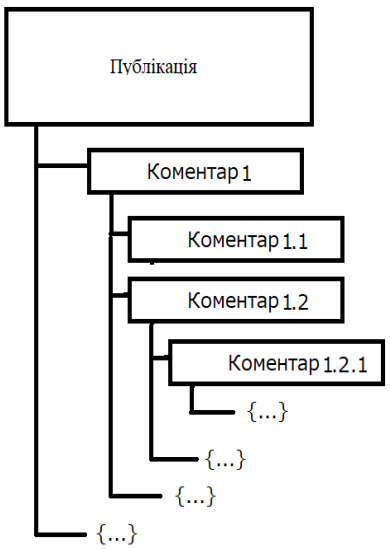

Рис. 3 – Схема принципу дерева вкладених коментарів

Також, на сучасних сайтах типу «блог», доволі часто розробники додають функції для створення відповідей, або цитування конкретних коментарів, або їх частин. Дані можливості підвищують конкретність висловлювань деякого користувача по відношенню до інших конкретних користувачів, або їх ідей.

Такі рішення дозволяють як організовувати спільні обговорення між учасниками веб–спільноти, так і отримувати зворотній зв'язок з автором публікації. Таким чином, автор може вносити зміни у публікацію, враховуючи усі важливі зауваження, критику та побажання, наведені у коментарях.

Системи, побудовані у вигляді форуму, перш за все мають чітку та розгалужену ієрархію гілок та обговорень. Саме чітка тематична організація комунікативної взаємодії користувачів сайту робить дану парадигму досить ефективною та популярною в організації веб–спільноти.

Основна взаємодія учасників форуму відбувається в обговореннях. Кожне обговорення повинно мати назву, а також містити не менше одного запису (посту). Члени віртуальної спільноти, які зацікавлені в обговоренні конкретної тематики, можуть залишати свої повідомлення, а також використовувати цитування або створювати «відповіді» конкретним учасникам дискусії.

Як і у випадку з блогом – користувачі можуть генерувати інформаційне наповнення згідно правил сайту. Таким чином, з точки зору документування, користувач може прикріпити текстовий файл, навести посилання на файл у мережі Інтернет, а також створити запис з контентом реального документа, за умови виконання встановлених правил сайту.

Соціальні мережі – доволі популярний вид організації віртуальних спільнот. Веб–ресурси даного типу можуть значною мірою відрізнятися за своїми функціональними та інструментальними особливостями. У більшості випадків, вони можуть поєднувати характерні ознаки багатьох розглянутих видів комунікативних веб–ресурсів, в залежності від функціонального призначення конкретної гілки сайту.

Слід зазначити, що популярні потужні соціальні мережі можуть мати як вбудовані засоби для забезпечення своїх функціональних можливостей (Pinterest), так і використовувати споріднені сервіси, які можуть бути використані окремо (Facebook, Google+).

Таким чином, кожна соціальна мережа може значно відрізнятися за принципами своєї роботи, використовуючи комбінації можливостей блогів, форумів, чатів, тощо. Також значною мірою може відрізнятись і архітектура кожної окремо взятої соціальної мережі. Але умовно можна описати основні принцип їх архітектурної реалізації.

Також набувають популярності системи, які не є соціальними мережами, але комбінують базові підходи декількох розглянутих типів сайтів всередині од-

ного, розширюючи свої функціональні можливості. Прикладами таких сайтів може служити “Habrahabr”, “Youtube”, “Lifehacker”. Дані ресурси мають функціональність блогу, як кінцевого результату, в той самий час підтримуючи певну категоризацію та авторство багатьох користувачів у межах свого сайту.

Архітектура та принципи функціонування як соціальних мереж, так і гібридних систем значною мірою можуть відрізнятися, в залежності від потреб у функціональних можливостях сервісу.

На основі запропонованих методів використання базових онлайн–спільнот у колаборативному документуванні, можна запропонувати розвиток поєднаних парадигм. Це може сприяти кращій організації процесу колаборації та документування. Якщо взяти до уваги сучасні можливості інтеграції сервісів різного типу у рамках одного веб–ресурсу, можливим стає використання саме тих функціональних можливостей, які особливо необхідні.

SWOT–аналіз результатів досліджень. Strengths. Сильні сторони даного дослідження полягають у тому, що запропоновані методи колаборативного документування доступні будь–яким користувачам у веб–просторі. Для реалізації даного процесу можливо використовувати вже існуючі веб–ресурси, які задовільняють потреби конкретної соціальної спільноти. Даний факт вказує на можливе скорочення або відсутність витрат, пов’язаних з побудовою нових сервісів з метою організації взаємодії всіх його учасників.

Weaknesses. До слабких сторін даного дослідження можна віднести малу ефективність деяких видів використання Інтернет–ресурсів. Це пов’язано з тим, що кожен тип сайту може мати дещо різну реалізацію, у порівнянні з класичними аналогами, а також мати як свої переваги так і недоліки. Навіть застосування соціальних мереж, або поєднаних парадигм у межах одного сайту може бути не раціональним, в залежності від способу їх використання та цільових потреб спільноти у цілому.

Opportunities. Згідно дослідження, процес колаборативного документування може бути реалізований різними типами веб–ресурсів. Найбільш перспективною тенденцією розвитку онлайн–спільнот з максимальними функціональними можливостями у даній галузі є створення систем на основі поєднання характерних парадигм класичних типів сайтів. Правильна реалізація поєднання характеристик класичних сайтів має можливість використання максимуму можливостей у рамках однієї інформаційної системи.

Threats. Складності в реалізації колаборативних можливостей заключаються в обмеженнях різних типів сервісів. Найбільш пристосованими, в даному питанні, є соціальні мережі та сервіси з поєднаними парадигмами. Такі підходи є найбільш прагматичними, проте іноді бувають також не вичерпними.

Також, для побудови нового веб–ресурсу необхідно правильно оформити концепцію та парадигми роботи, згідно основного цільового призначення. Крім того, реалізація нового сервісу потребує витрат часу та матеріальних ресурсів.

Висновки. Методи організації колаборативного документування, запропоновані у даному дослідженні мають свої особливості застосування. У ході аналізу типових можливостей веб–ресурсів кожного з видів онлайн–спільнот було отримано декілька можливих сценаріїв, за якими користувачі можуть здійснювати колаборативну взаємодію у рамках конкретного сайту, при роботі з електронними документами.

Чати мають найменшу перевагу серед інших систем. Їх сильна сторона полягає у тому, що вони можуть бути реалізовані у якості допоміжного інструмента для підвищення комунікативних можливостей учасників віртуальної спільноти. У такому випадку, користувачі матимуть можливість активного онлайн–обговорення при безпосередній роботі над основним завданням.

Блоги дозволяють доволі активно поширювати контент, а також файли у веб–середовищі. За допомогою коментарів можливий зворотній зв’язок з іншими користувачами. Існують, у деяких випадках, засоби вкладених коментарів, цитування та створення «відповіді», що робить комунікації більш зручними. Важливо, що дана парадигма у класичному вигляді вказує на авторство публікацій однією людиною, з відсутністю серйозних ієрархічних розділів, тому вона не є завжди зручною.

Форуми складаються зі складних ієрархічних гілок та обговорень, які мають налаштовані права доступу до них. Також вони містять майже усі можливості блогу, з точки зору роботи з електронними документами. Саме ці характеристики роблять форуми популярними для організації колаборативних процесів, адже користувачі, на відміну від блогу, можуть створювати свої обговорення та гілки, якщо це дозволено адміністраторами сайту.

Соціальні мережі мають різну мету та особливості їх функціональної реалізації. В основному, соціальні мережі об’єднують у собі декілька парадигм для досягнення максимальних цілей.

Застосування ресурсів, що поєднують у собі парадигми декількох класичних видів систем дозволяє використовувати найбільш ефективно усі можливості, у випадку, якщо це раціонально реалізовано/

В результаті виконаного аналізу, було запропоновано найбільш ефективні методи використання кожного з досліджуваних типів веб–ресурсів у процесі колаборативного документування між учасниками веб–спільнот. Було виявлено, що сервіси з поєднаними моделями є найбільш ефективними, за рахунок реалізації максимальних функціональних можливостей у рамках однієї інформаційної системи.

Таким чином, внаслідок даного дослідження моделей онлайн–спільнот, було виявлено можливі методи використання різних типів веб–ресурсів у процесі колаборативного документування, які можуть бути доступними широкому загалу людей. Найбільш перспективними, у плані розвитку, є системи з поєднаними парадигмами. Саме такі системи дозволяють об’єднувати у собі класичні моделі досліджених веб–ресурсів, забезпечуючи кращу ефективність організації взаємодії між учасниками спільноти.

Список літератури:

1. *Пелещишин, А. М.* Процеси управління інтерактивними соціальними комунікаціями в умовах розвитку інформаційного суспільства [Текст]: монографія / *А. М. Пелещишин, Ю. О. Сєров, О. Л. Березко, О. П. Пелещишин, О. Ю. Тимовчак-Максимець, О. В. Марковець*. – Львів: Видавництво Національного університету «Львівської політехніка», 2011. – 374 с.
2. *Пелещишин, А. М.* Аналіз існуючих типів віртуальних спільнот у мережі Інтернет та побудова моделі віртуальної спільноти на основі веб-форуму [Текст] / *А. М. Пелещишин, Р. Б. Кравець, Ю. О. Сєров* // Вісник Національного університету "Львівська політехніка". – 2011. – № 699. – С. 212–221.
3. *Peleschyshyn, A.* Typical ways of web communities development [Text] / *A. Peleschyshyn, Yu. Syerov* // Proceedings of the International Conference on Computer Science and Information Technologies. – Lviv, 2006. – P. 56–58.
4. *Федушко, С. С.* Моделювання структури та функціонування спеціалізованої віртуальної спільноти на основі блогу (на прикладі webstyletalk.net) [Текст] / *С. С. Федушко, М. О. Котило, Ю. О. Сєров* // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2012. – № 2 (173). – С. 150–155.
5. *Кравець, Р. Б.* Дослідження поведінки учасників веб-спільнот та їх класифікація [Текст] / *Р. Б. Кравець, А. М. Пелещишин, Ю. О. Сєров* // Вісник Національного університету "Львівська політехніка". – 2008. – № 621. – С. 153–161.
6. *Тимовчак-Максимець, О. Ю.* Аналіз комунікативної взаємодії на веб-форумах: інформаційна поведінка та учасники [Текст] / *О. Ю. Тимовчак-Максимець, А. М. Пелещишин, К. О. Слобода* // Вісник Національного університету "Львівська політехніка". – 2011. – № 699. – С. 352–361.
7. *Федушко, С. С.* Аналіз архітектури та сучасних тенденцій розвитку віртуальних спільнот [Текст] / *С. С. Федушко* // Вісник Національного університету "Львівська політехніка". – 2011. – № 699. – С. 362–375.
8. *Вершинин, А. П.* Электронный документ: правовая форма и доказательство в суде [Текст] / *А. П. Вершинин.* – М., 2000. – С. 40.
9. *Годин, В. В.* Управление информационными ресурсами: 17-ти модульная программа для менеджеров «Управление развитием организации» [Текст] / *В. В. Годин, И. К. Корнеев*. – М., 2000. – С. 15.
10. *Залаев, Г. З.* Анализ и классификация электронных документов [Текст] / *Г. З. Залаев* // Вестник архивиста. – 1999. – № 2-3. – С. 60–68.
11. *Бачило, И. Л.* Правовые вопросы документирования в условиях информатизации [Текст] / *И. Л. Бачило* // Делопроизводство. – 1998. – № 2. – С. 13.
12. *Костомаров, М. И.* Многоликий Янус: документ в системе информационного менеджмента [Текст] / *М. И. Костомаров* // Делопроизводство. – 1998. – № 1. – С. 29.
13. *Ларин, М. В.* Некоторые проблемы эволюции управленческого документа [Текст] / *М. В. Ларин* // Доклад на 6-й научно-практической конференции. – 1999.
14. *Ткачев, Л. В.* Правовой статус компьютерных документов: основные характеристики [Текст] / *Л. В. Ткачев.* – М., 2000. – С. 8.
15. *Mulesa, O.* Information technology for determining structure of social group based on fuzzy c-means [Text] / *O. Mulesa, F. Geche, A. Batyuk* // 2015 Xth International Scientific and Technical Conference "Computer Sciences and Information Technologies" (CSIT). – 2015. doi: 10.1109/stc-csit.2015.7325431
16. *Biloshchytskyi, A.* A method for the identification of scientists' research areas based on a cluster analysis of scientific publications [Text] / *A. Biloshchytskyi, A. Kuchansky, Y. Andrashko, S. Biloshchytska, O. Kuzka, Y. Shabala, T. Lyashchenko* // Eastern-European Journal of Enterprise Technologies. – 2017. – Vol. 5, Issue 2 (89). – P. 4–11. doi: 10.15587/1729-4061.2017.112323

Bibliography (transliterated):

1. Peleshchyshyn, A. M., Sierov, Yu. O., Berezko, O. L., Peleshchyshyn, O. P., Tymovchak-Maksymets, O. Yu., Markovets, O. V. (2011). Protsesy upravlinnia interaktyvnymy sotsialnymy komunikatsiiamy v umovakh rozvytku informatsiinoho suspilstva. Lviv: Vydavnytstvo Natsionalnoho universytetu «Lvivskoi politekhnika», 374.
2. Peleshchyshyn, A. M., Kravets, R. B., Sierov, Yu. O. (2011). Analiz isnuiuchykh typiv virtualnykh spilnot u merezhi Internet ta pobudova modeli virtualnoi spilnoty na osnovi veb-forumu. Visnyk Natsionalnoho universytetu "Lvivska politekhnika", 699, 212–221.
3. Peleschyshyn, A., Syerov, Yu. (2006). Typical ways of web communities development. Proceedings of the International Conference on Computer Science and Information Technologies. Lviv, 56–58.
4. Fedushko, S. S., Kotylo, M. O., Sierov, Yu. O. (2012). Modeliuvannia struktury ta funktsionuvannia spetsializovanoi virtualnoi spilnoty na osnovi blogu (na prykladi webstyletalk.net). Visnyk Skhidnoukrainskoho natsionalnoho universytetu imeni Volodymyra Dalia, 2 (173), 150–155.
5. Kravets, R. B., Peleshchyshyn, A. M., Sierov, Yu. O. (2008). Doslidzhennia povedinky uchasnykiv veb-spilnot ta yikh klasyfikatsiya. Visnyk Natsionalnoho universytetu "Lvivska politekhnika", 621, 153–161.
6. Tymovchak-Maksymets, O. Yu., Peleshchyshyn, A. M., Sloboda, K. O. (2011). Analiz komunikatyvnoi vzaiemodii na veb-forumakh: informatsiina povedinka ta uchasnyky. Visnyk Natsionalnoho universytetu "Lvivska politekhnika", 699, 352–361.
7. Fedushko, S. S. (2011). Analiz arkhitektury ta suchasnykh tendentsii rozvytku virtualnykh spilnot. Visnyk Natsionalnoho universytetu "Lvivska politekhnika", 699, 362–375.
8. Vershinin, A. P. (2000). Elektronnyy dokument: pravovaya forma i dokazatel'stvo v sude. Moscow, 40.
9. Godin, V. V., Korneev, I. K. (2000). Upravlenie informacionnymi resursami: 17-ti modul'naya programma dlya menedzherov «Upravlenie razvitiem organizacii». Moscow, 15.
10. Zalaev, G. Z. (1999). Analiz i klassifikaciya elektronnyh dokumentov. Vestnik arhivista, 2-3, 60–68.
11. Bachilo, I. L. (1998). Pravovye voprosy dokumentirovaniya v usloviyah informatizacii. Deloproizvodstvo, 2, 13.
12. Kostomarov, M. I. (1998). Mnogolikiy Yanus: dokument v sisteme informacionnogo menedzhmenta. Deloproizvodstvo, 1, 29.
13. Larin, M. V. (1999). Nekotorye problemy evolyucii upravlencheskogo dokumenta. Doklad na 6-y nauchno-prakticheskoy konferencii.
14. Tkachev, L. V. (2000). Pravovoy status komp'yuternyh dokumentov: osnovnye harakteristiki. Moscow, 8.
15. Mulesa, O., Geche, F., Batyuk, A. (2015). Information technology for determining structure of social group based on fuzzy c-means. 2015 Xth International Scientific and Technical Conference "Computer Sciences and Information Technologies" (CSIT). doi: 10.1109/stc-csit.2015.7325431
16. Biloshchytskyi, A., Kuchansky, A., Andrashko, Y., Biloshchytska, S., Kuzka, O., Shabala, Y., Lyashchenko, T. (2017). A method for the identification of scientists' research areas based on a cluster analysis of scientific publications. Eastern-European Journal of Enterprise Technologies, 5 (2 (89)), 4–11. doi: 10.15587/1729-4061.2017.112323

Надійшла (received) 02.12.2017

Бібліографічні описи / Библиографические описания / Bibliographic descriptions

Моделі онлайн–спільнот як основа взаємодії учасників колаборативного документування/ Гетманюк П. О., Форкун Ю. В. //Bulletin of NTU "KhPI". Series: Mechanical-technological systems and complexes. – Kharkov: NTU "KhPI", 2017. – № 44 (1266).– P.85–90. – Bibliogr.:16. – ISSN 2079-5459

Модели онлайн–сообществ как основа взаимодействия учасников колаборативного документирования/ Гетманюк П. О., Форкун Ю. В. //Bulletin of NTU "KhPI". Series: Mechanical-technological systems and complexes. – Kharkov: NTU "KhPI", 2017. – № 44 (1266).– P.85–90. – Bibliogr.:16. – ISSN 2079-5459

Models of online–communities as a communicational basis in collaborative documentation/ Getmanyk P., Forkun Y. //Bulletin of NTU "KhPI". Series: Mechanical-technological systems and complexes. – Kharkov: NTU "KhPI", 2017. – № 44 (1266).– P.85–90. – Bibliogr.:16. – ISSN 2079-5459

Відомості про авторів / Сведения об авторах / About the Authors

Гетманюк Павло Олександрович – Аспірант, Кафедра інженерії програмного забезпечення, Хмельницький національний університет, вул. Інститутська 11, Хмельницький, Україна, 29000, E–mail: gornnaemnik@gmail.com.

Форкун Юрій Вікторович – Кандидат технічних наук, доцент, Кафедра інженерії програмного забезпечення, Хмельницький національний університет, вул. Інститутська 11, Хмельницький, Україна, 29000, E–mail: forkun@ridne.net.

Гетманюк Павел Александрович – Аспирант, Кафедра инженерии програмного обеспечения, Хмельницкий национальный університет, вул. Институтская 11, Хмельницкий, Украина, 29000,

Форкун Юрий Викторович – кандидат технических наук, доцент, Кафедра инженерии програмного обеспечения, Хмельницкий национальный університет, вул. Институтская 11, Хмельницкий, Украина, 29000,

Getmanyuk Pavlo – postgraduated student, Department Software Engineering, Khmelnitskiy national university, str. Institutska 11, Khmelnitskiy, Ukraine, 29000, e–mail: gornnaemnik@gmail.com.

Forkun Iurii – PhD., associate professor, Department Software Engineering, Khmelnitskiy national university, str. Institutska 11, Khmelnitskiy, Ukraine, 29000, e–mail: forkun@ridne.net.

УДК 681.3

Р. В. СКУРАТОВСКИЙ, Е. О. ОСАДЧИЙ, Д. М. КВАШУК

ДЕЛЕНИЕ ТОЧКИ СКРУЧЕННОЙ КРИВОЙ ЭДВАРДСА НА ДВА И ЕГО ПРИМЕНЕНИЕ В КРИПТОГРАФИИ

Большинство криптосистем современной криптографии естественным образом можно реализовать на эллиптических кривых. Мы рассматриваем алгебраические кривые в форме Эдвардса над простым полем, F_p, которые сейчас являются одними из наиболее перспективных носителей групп, используемых в асимметричных криптосистемах. Показано, что проективная кривая Эдвардса $E_{a,d}$ не является эллиптической. Исследовано некоторые интересные свойства группы точек этих кривых. Найдено род скрученной кривой Эдвардса и ее особые точки. Показано возможность построения генератора случайных крипто стойких последовательностей на этой кривой. Предложена нормализация скрученной кривой Эдвардса. Исследованы условия делимости на два элемента из группы точек скрученной кривой Эдвардса над полем F_{p^n} . Целью роботы есть поиск критерия делимости точки кривой напополам над полем F_{p^n} и анализ свойств скрученной кривой Эдвардса необходимых для построения генератора псевдослучайных крипто стойких последовательностей.

Ключевые слова: конечное поле, алгебраическая кривая, группа точек эллиптической кривой, делимость точки кривой пополам.

Більшість криптосистем сучасної криптографії природним чином можна реалізувати на еліптичні криві. Ми розглядаємо алгебраїчні криві Едвардса над скінченним полем F_{p^n} , які на даний час є одним з найбільш перспективних носіїв множин точок, що використовують для швидких групових операцій, які наявні в асиметричних криптосистемах, зокрема для побудови випадкових криптостійких послідовностей. Показано, що проективна крива $E_{a,d}$ не є еліптичною. Досліджено умови існування подільності навпіл елемента з групи точок скрученої кривої Едвардса $E_{a,d}$, що є важливим в алгоритмах. Знайдено рід скрученої кривої Едвардса. Метою роботи є пошук критерію подільності точки кривої навпіл над полем F_{p^n} і аналіз властивостей скрученої кривої Едвардса необхідних для побудови генератора псевдовипадкових криптостійких послідовностей і побудова односторонньої функції для нього.

Ключові слова: скінчене поле, алгебраїчна крива, група точок еліптичної кривої, подільність точки кривої навпіл.

Most cryptosystems of modern cryptography can be naturally transformed into elliptic curves. We review Edwards algebraic curves over a finite field, which at the present time is one of the most promising carriers of sets of points that are used for fast group operations. These are found in asymmetric cryptosystems. In particular, for constructing random crypto-stable sequences. It is shown that the projective curve is not elliptic.

The conditions of the existence of divisibility in half an element from the group of points of the twisted curve of Edwards $E_{a,d}$, which is important in algorithms, are investigated. The type of twisted curve Edwards is found. The purpose of the work is to find the criterion of the divisibility of the point of the curve in half over the field and to analyze the properties of the twisted curve of Edwards necessary for constructing a generator of pseudo-random crypto-stable sequences and constructing a one-way function F_{p^n} for it.

Keywords: finite field, elliptic curve, Edwards curve, order of a curve, finite field, algebraic curve, group of points of an elliptic curve, order of a point, torsion curves.