УДК 004.891

к.т.н., доц. **Бойчук В.О.** (ХмНУ)
Юмашов В.С. (ХмНУ)

МЕТОД ВИЯВЛЕННЯ ЗАГРОЗИ ПОШИРЕННЯ ЗАБОРОНЕНОЇ ДО РОЗПОВСЮДЖЕННЯ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

У статті розглядаються комп'ютерні мережі (КМ), що знаходяться під впливом загрози поширення забороненої інформації. Досліджуються моделі загрози поширення цієї інформації і особливості комп'ютерних мереж. Наведено основні проблеми інформаційної безпеки, які актуальні для даного дослідження і алгоритм по якому здійснюється функціонування комп'ютерних мереж, що знаходяться під впливом загрози поширення забороненої інформації.. З бурхливим ростом числа користувачів КМ виникають проблеми інформаційної безпеки і захисту інформації в них. Аналіз цих проблем виявив, що існує маловивчена проблема забороненого контенту. Створення моделей і алгоритмів поширення загрози забороненої інформації – один з ключових підходів при вирішенні даного завдання.

Ключові слова: безпека комп'ютерних мереж, заборонена інформація, велика чисельність користувачів, моделювання.

Вступ. Комп'ютерні мережі (КМ) забезпечують практично повний спектр можливостей для обміну інформацією між користувачами - мережевими абонентами. Комп'ютерна мережа

надає різні сервіси для організації соціальних взаємовідносин між користувачами (абонентами). На сьогоднішній день найбільш популярним з них є соціальні мережі. У світі існує величезна кількість різних соціальних мереж, але практично в кожній країні або регіоні існують кілька найбільш популярних представників. У США це «Facebook», «MySpace», «Twitter» і «LinkedIn»; «Nexopia» - в Канаді, «Bebo» - в Великобританії, «Facebook», «dol2day» - в Німеччині. В Україні на сьогоднішній день найпопулярними є «ВКонтакте» і «Однокласники». Сучасною проблемою таких систем є їх низький рівень інформаційної безпеки. Для забезпечення захисту інформації в телекомунікаційних мережах, включаючи Інтернет, розроблено безліч методів і засобів, запропонованих в працях П.Д. Зегжди, С.П. Расторгуєва, Р. Бретта, В.І. Завгороднього, В.А. Герасименко, А.А. Малюка, В. Столінгса, К. Касперски, С. Норкатта, В.В. Домарева. Тим не менш, ефективного захисту абонентів від загроз поширення забороненої інформації, зокрема в умовах широкого використання індивідуально-орієнтованих сервісів і пов'язаних з ними протоколів і технологій (SOAP, CORBA, REST і ін.), не існує. Серед безлічі функцій захисту принциповою відносно цих систем є функція попередження прояву забороненої інформації. Вона реалізується за рахунок механізмів прогнозування загрози поширення і розсилки повідомлень з попередженнями про наслідки дій із забороненим контентом. Використання інших функцій (попередження, виявлення, локалізації та ліквідації загрози) припускає наявність повного контролю над системою, що в справжніх умовах неможливо.

Постановка задачі. Одним з підходів до прогнозування загрози поширення забороненої інформації (ЗгЗІ) є моделювання, наприклад, з використанням моделей впливу, моделей просочування і зараження (Д.А. Новиков, Д.А. Губанов і А.Г. Чхартішвілі, J. Leveille, D . Watts і S. Strogatz, R. Albert та A. Barabasi, J. Leskovec, M. Gjoka, SN Dorogovtsev, MEJ Newman і RM Ziff, JO Kephart і SR White і ін.). Дані моделі, як правило, не враховують топологічні особливості мережі (розподіл ступенів зв'язності, кластерний коефіцієнт, середня довжина шляху). Взаємодія між абонентами в рамках цих математичних моделей описується переважно гомогенним графом, що при моделюванні великомасштабних мереж (більше 10 млн. вузлів) може дати похибку прогнозування ЗгЗІ більше 30%. Крім того, дані підходи носять в основному теоретичний характер, практика їх використання не виходить за рамки експериментів. Таким чином, дослідження, спрямовані на створення моделей та алгоритмів ЗгЗІ, актуальні і мають теоретичне і практичне значення у вирішенні проблеми забезпечення інформаційної безпеки в системах і мережах телекомунікацій.

Мета роботи полягає в підвищенні точності прогнозування загрози поширення забороненої інформації в комп’ютерних мережах.

Для досягнення мети роботи необхідно вирішити наступні завдання:

1. Провести інформаційний огляд і експерименти для виявлення істотних характеристик об'єкта і зовнішніх факторів, що впливають на процес реалізації ЗгЗІ. Виконати аналіз основних підходів до моделювання ЗгЗІ.

2. Розробити імітаційну модель ЗгЗІ в КМ.

3. Синтезувати і показати адекватність аналітичної моделі ЗгЗІ в КМ.

4. Розробити методику формування топології КМ.

5. Змоделювати процес реалізації ЗгЗІ на топології реальної великомасштабної КМ. Провести експериментальне дослідження з отриманими результатами.

Виклад основного матеріалу досліджень. Узагальнена структурна схема КМ приведена на рис. 1. Її склад в загальному випадку утворюють такі елементи:

- Абоненти (А) – людино-машинні системи, що складаються з пристрою, через який здійснюється доступ до мережі, і безпосередньо користувача. Абоненти можуть бути окремими вузлами мережі (якщо користувач використовує свій домашній комп'ютер), або можуть бути об'єднані в корпоративну обчислювальну мережу (КОМ), включають в себе модулі (інформаційного) захисту (МЗ) і програмне забезпечення (браузер) для взаємодії з керуючим елементом;

- Мобільні абоненти (МА). Користувачі, які використовують мобільні пристрої (смартфони, планшети і тд.), Для доступу до мережі. Також використовують програмне забезпечення (спеціальний додаток) і МЗ;

- Сервери (С). У КОМ знаходяться інформаційні сервери різного функціонального призначення, які беруть участь в інформаційній взаємодії (наприклад, проксі-сервера);

- КОМ включає в себе крім абонентів і серверів, також засоби маршрутизації, комутації та адміністрування (МКА), систему безпеки (СБ), що включає механізми захисту для всієї корпоративної мережі;

- Засоби телекомунікації, що забезпечують взаємодію між абонентами;

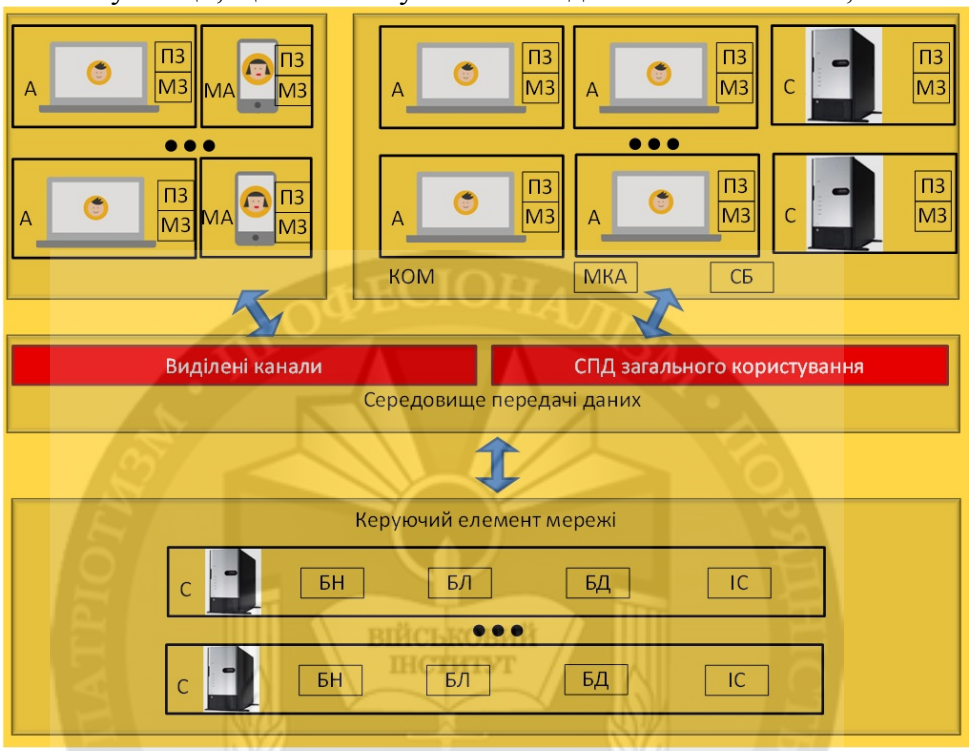

Рис. Структурна схема КМ

- Керуючий елемент технічно являє собою сукупність комутуючого і серверного устаткування, що реалізує основні функції системи. Включає в себе сервери, які містять в загальному випадку: балансувальник навантаження (БН), елемент бізнес-логіки (БЛ), бази даних (БД), інфраструктурні системи (ІС) (системи статистики, конфігурації, моніторингу і тд.).

Особливості КМ:

1) Абонентами є людино-машинні системи. Спосіб взаємодії абонентів – смислові повідомлення. Рішення про взаємодію приймається користувачами.

2) Постійно змінюється число абонентів і зв'язків між ними.

3) Складність процедури ідентифікації абонентів і віднесення повідомлення до забороненої інформації.

4) Складність реалізації захисту. Основний спосіб її реалізації - попередження абонента про відповідальність за поширення забороненої інформації.

5) Особливості програмно-логічної організації КМ (наприклад, соціальні мережі «ВКонтакте» і «Facebook»), які призводять до неминучого отримання повідомлення абонентом при наявності зв'язку між ним і абонентом-зловмисником.

6) Великомасштабність - КМ, як правило, містять мільйони абонентів.

7) Основною проблемою КМ, крім проблем, пов'язаних з використанням глобальної мережі Інтернет, є проблема забороненої інформації.

Функціонування КМ, що знаходиться під впливом ЗгЗІ, здійснюється за наступним алгоритмом.

Крок 1. Поширення забороненої інформації (ЗІ) (далі процес «атаки») ініціює будь-який абонент-зловмисник, поширюючи повідомлення з ЗІ (реалізує загрозу) по його списку контактів. Атаку може починати один зловмисник або група.

Крок 2. Абоненти-одержувачі, прийнявши повідомлення з ЗІ, читають його і включаються в процес атаки, поширюючи її далі по своїм контактам, або ігнорують або взагалі видаляють повідомлення, тобто в атаці не беруть участь. Процес атаки зазвичай йде лавиноподібно. Атакуючі абоненти не закінчують атаку, одного разу передавши повідомлення із забороненою інформацією. Вікно атаки, як правило, триває протягом досить значного проміжку часу і залежить від типу подачі ЗІ в повідомленні, зацікавленості абонента і тд.

Крок 3. Абоненти-зловмисники можуть перестати розповсюджувати і, відповідно, сприймати ЗІ (далі процес «захисту»), внаслідок впливу механізмів захисту (наприклад, попередження про нього), тому повідомлення з ЗІ від атакуючих абонентів будуть постійно відхилятися.

Крок 4. Процес триває поки в мережі є абоненти-зловмисники, або є потенційно вразливі вузли, якщо відсутній процес захисту.

Один з ключових підходів при вирішенні проблеми ЗІ - створення моделей і алгоритмів ЗгЗІ. Проведений аналіз показує, що існуючі рішення малоефективні. При моделюванні ЗгЗІ не враховується топологія КМ (модель мережі - повнозв'язний граф). А, якщо топологія враховується, то, як правило, використовується найпростіша SIS модель, а структура мережі відображається Scale-Free або Small world мережею. При моделюванні ЗгЗІ важливо мати топологію, яка відображатиме структуру зв'язків реальної мережі, а також використовувати коректну модель інформаційної взаємодії вузлів.

Концептуальна математична модель інформаційної взаємодії абонентів представляється графом, вершинами якого є абоненти, а ребрами - зв'язки між ними. Відзначимо властивості графа, принципові для справжнього дослідження: велика розмірність, гетерогенність, динаміка зв'язків і вузлів, наявність груп вузлів, що мають велику кількість зв'язків усередині кластера і невелике - між ними.

З аналізу предметної області можна зробити висновок про те, що на процес реалізації ЗгЗІ в КМ істотно впливають мережеві структурні характеристики (топологія). Отримання структури соціальної мережі пов'язано з вибіркою вузлів з неї, що само по собі вже є нетривіальним завданням, так як вибірка повинна відображати властивості всієї мережі в цілому, тобто бути репрезентативною.

Таким чином, для підвищення точності прогнозування ЗгЗІ в КМ потрібно:

1. розробити імітаційну модель ЗгЗІ, що враховує топологічні характеристики і особливості інформаційної взаємодії абонентів як людино-машинних систем;

2. розробити аналітичну модель реалізації ЗгЗІ, що враховує характеристики вразливості КМ і дозволяє підвищити точність оперативного прогнозу в умовах неповноти вихідних даних про топологію мережі;

3. експериментально підтвердити адекватність аналітичної моделі, змоделювавши процес реалізації ЗгЗІ на топології великомасштабної мережі.

Наведемо основні проблеми інформаційної безпеки в КМ, які актуальні для даного дослідження.

1. Використання глобальної мережі Інтернет як розподіленої комп’ютерної системи.

Найбільш вразливими і тому часто яких атакують компонентами системи є:

1) Сервери.

2) Робочі станції.

3) Середовище передачі інформації.

4) Вузли комутації.

Типові інформаційні впливи зловмисників:

1) Прослуховування мережевого трафіку. Для прослуховування трафіку (sniffing) мережевий адаптер переводиться в «безладний» режим. В даному режимі адаптер перехоплює всі мережеві пакети, що проходять через нього, а не тільки призначені даній адресі, як в нормальному режимі функціонування-технології - ARP Spoofing (ARP-poisoning), MAC Flooding і MAC Duplicating. Перехоплення здійснюється з використанням мережевих моніторів, з яких найбільш функціональними є Sniffer Pro від компанії Sniffer Technologies, IRIS Network Traffic Analyzer від компанії eEYE і TCP Dump.

Наслідки. Сучасні мережеві протоколи (TCP / IP, ARP, HTTP, FTP, SMTP, POP3 і т.д.) не мають механізмів захисту (передаються у відкритому вигляді). Зловмисник, що перехоплює трафік між сервером і будь-яким вузлом мережі, може заволодіти аутентифікаційними даними користувача (отримати пароль).

Протидія. Відомий ряд методів визначення наявності запущеного сніффер в мережі, наприклад, метод пінга, метод ARP, метод DNS і метод пастки.

2) Сканування вразливостей. Результатом роботи сканера є інформація про систему, що включає список мережевого обладнання, комп'ютерів з запущеними на них службами, версіями мережевого ПО (а значить і вразливостей, властивих даному ПО), облікові записи користувачів. Сканування вразливостей зазвичай є етапом, що передує атаці. Саме результати сканування дозволяють точно підібрати експлойти для здійснення безпосередньо несанкціонованого доступу.

Виявлення. Само по собі сканування не є незаконним. Однак, якщо сканування з боку зовнішньої, по відношенню до системи, мережі звичайне явище, то сканування комп'ютерів з внутрішньої мережі - безумовно, інцидент безпеки, що вимагає негайної реакції з боку мережевого адміністратора. Виявити сліди сканування можна, вивчаючи журнали реєстрації міжмережевого екрану (МЕ). Однак такий підхід не дозволяє своєчасно реагувати на подібні інциденти. Тому сучасні МЕ і системи виявлення вторгнень (СВВ) мають модулі (plug-in), що дозволяють виявити сканування в режимі реального часу. Деякі сканери вразливостей використовують оригінальні методи, що дозволяють виробляти сканування максимально приховано. Наприклад, в Nmap існують можливості, що дозволяють значно ускладнити виявлення сканування для СВВ.

Протидія. Використання мережевих СВВ, або періодичне вивчення журналів реєстрації МЕ.

3) Мережеві атаки. Мережеві атаки можна розділити на:

- атаки, засновані на переповненні буфера (overflow based attacks). Вони використовують вразливість системи, яка полягає в некоректній програмній обробці даних. При цьому з'являється можливість виконання небезпечного коду з підвищеними привілегіями;

- атаки, спрямовані на відмову в обслуговуванні (Denial Of Service attacks). Атаки не обов'язково використовують вразливості в ПЗ системи що атакується. Порушення працездатності системи відбувається через те, що дані які їй посилають призводять до значної витрати ресурсів системи. Найпростішим прикладом атаки цього типу є атака «Ping Of Death». Суть її в наступному: на машину жертви надсилається сильно фрагментований ICMP-пакет великого розміру (64KB). Реакцією ОС Windows на отримання такого пакету є повне зависання.

4) Атаки, засновані на використанні вразливостей в ПЗ мережевих додатків - експлойти (exploit). Даний клас атак заснований на експлуатації різних дефектів в ПЗ. Експлойти представляють собою небезпечні програми, що реалізують відому вразливість в ОС або прикладному ПЗ, для отримання несанкціонованого доступу до вразливого хосту або порушення його працездатності. Для експлойтів характерна наявність функцій придушення антивірусних програм і МЕ. Наслідки застосування експлойтів можуть бути найкритичнішими. У разі отримання зловмисником віддаленого доступу до системи, він має практично повний (системний) доступ до комп'ютера. Наступні дії і збиток від них можуть бути наступними: впровадження троянської програми, впровадження набору утиліт для

приховування факту компрометації системи, несанкціоноване копіювання зловмисником даних з жорстких і змінних носіїв інформації системи, створення на віддаленому комп'ютері нових облікових записів з будь-якими правами в системі для подальшого доступу як віддалено, так і локально, крадіжка файлу з хешами паролів користувачів, знищення або модифікація інформації, здійснення дій від імені користувача системи.

Протидія. МЕ і СВВ, встановлені на системі що атакується, в ряді випадків не в змозі відобразити дію експлойтів. Для успішного відбиття атак експлойтів засоби захисту необхідно оновлювати, оскільки механізм виявлення вторгнень заснований на розпізнаванні сигнатур вже відомих атак. Хоча існують розробки, здатні по завіреннях розробників відображати невідомі атаки, практика показує, що вони все ще не ефективні.

5) Небезпечні програми (НПр). НПр - це комп'ютерна програма або переносний код, призначений для реалізації загроз інформації, що зберігається в мережі, або для прихованого нецільового використання ресурсів або якогось іншого впливу, що перешкоджає нормальному функціонуванню мережі. До НПр відносяться комп'ютерні віруси, троянські коні, мережеві черв'яки і ін.

Протидія. Типовим методом протидії є використання антивірусних засобів, що працюють в режимі реального часу (моніторів). Для виявлення троянських програм існує спеціалізоване програмне забезпечення.

2. Проблема забороненого контенту.

Залежно від законодавства країни різні матеріали можуть вважатися нелегальними. У більшості країн заборонені: матеріали сексуального характеру за участю дітей і підлітків, порнографічний контент, опису насильства, в тому числі сексуального, екстремізм і розпалювання расової ненависті.

В українському законодавстві існує поняття захисту суспільної моралі. Визначається така інформація постановою уряду України, від 20 листопада 2003 року в законі України Про захист суспільної моралі та законом Про внесення змін до Закону України «Про захист суспільної моралі» від 10 лютого 2015 року. В постанові докладно вказано, яка інформація визнана незаконною до поширення в Україні в мережі Інтернет, і які правоохоронні органи відповідальні за контроль над поширенням незаконної інформації.

Захист суспільної моралі полягає у здійсненні діяльності органами державної влади і місцевого самоврядування, у тому числі за участю громадських організацій, спрямованої на попередження і недопущення розповсюдження продукції та показу видовищних заходів, які завдають шкоди суспільній моралі.

Метою державної політики у сфері захисту суспільної моралі є формування єдиної комплексної громадсько-державної системи забезпечення захисту моральних засад і утвердження мотивації українського суспільства на здоровий спосіб життя, недопущення в електронних та інших засобах масової інформації культу насильства та жорстокості, поширення продукції порнографічного характеру, расової і національної ворожнечі, фашизму, неофашизму, ксенофобії, українофобії, антисемітизму, нетерпимості, образи нації чи особи за національною ознакою тощо.

Аналогічно з концепцією забезпечення комплексного захисту об'єкта інформатизації, можна сформувати повну множину функцій захисту від забороненої інформації.

Під функцією захисту (ФЗ) розуміється сукупність однорідних в функціональному відношенні заходів, регулярно здійснюваних в автоматизованих системах різними засобами і методами з метою створення, підтримки і забезпечення умов, об'єктивно необхідних для надійного захисту інформації.

Перелік числа функцій захисту від забороненої інформації в соціальних мережах:

1) Попередження умов виникнення забороненої інформації.

Функція реалізується за допомогою нормативно-правових актів. Вона не може повністю виключити загрозу поширення забороненої інформації в соціальних мережах, так як в цілому ситуація з дотриманням законів (особливо в Україні) незадовільна, а в інтернет-просторі загострюється через технічні складнощі.

2) Попередження безпосереднього проявлення забороненої інформації.

Функція реалізується за рахунок механізмів прогнозування поширення забороненої інформації в соціальній мережі. Більш детально дана функція буде розглянута пізніше.

3) Виявлення забороненої інформації яка проявилася.

Функція пов'язана з моніторингом КМ на предмет забороненої інформації на сторінках абонентів. Як правило, реалізація даного захисту виконується уповноваженими органами оперативно-розшукових заходів у телекомунікаційних мережах загального користування України. Дана ФЗ пов'язана з проблемами контекстного пошуку, а також необхідністю контролю над всією системою.

4) Попередження впливу на абонентів забороненої інформації яка проявилася.

Функція може бути реалізована за допомогою автоматичної розсилки повідомлень з попередженням про відповідальність за поширення забороненої інформації, аж до блокування абонента. Блокування може здійснюватися легітимними засобами за наявності доступу до управління системи і нелегітимними - при його відсутності (злом акаунта). ФЗ ділиться на дві функції (ФЗ4а і ФЗ4б). Перша пов'язана з попередженням абонентів, на сторінках яких була знайдена заборонена інформація, а друга – з розсилкою попереджень потенційним отримувачам забороненої інформації.

5) Виявлення впливу забороненої інформації на абонентів.

Функція пов'язана безпосередньо з фіксацією процесу поширення забороненої інформації, може бути реалізована через контекстний аналіз повідомлень. Властиві такі ж недоліки, як і для ФЗ3.

6) Локалізація, обмеження впливу забороненої інформації на абонентів.

Функція реалізується через блокування абонентів, що поширюють заборонену інформацію (ФЗ6а), або абонентів – потенційних розповсюджувачів (ФЗ6б). Дана ФЗ спирається на попередні функції і для її ефективної реалізації необхідний контроль над системою.

7) Ліквідація наслідків виявленого впливу забороненої інформації на абонентів.

Функція пов'язана з видаленням забороненої інформації з системи. Для реалізації даної функції також необхідний контроль над системою.

На рис. 2 наведено всі поєднання подій, які потенційно можливі при здійсненні всіх ФЗ.

Рис. Функції захисту від забороненої інформації в КМ

З аналізу функцій захисту видно, що найбільш ефективні функції - це перші функції, так як вони забезпечують захист на ранніх етапах. Всі функції мають свої недоліки. Найбільш перспективною ФЗ інженерно-технічного напряму є ФЗ2. Саме їй присвячена дана робота. На даному етапі, маючи інформацію про топології КМ і потенційних розповсюджувачів забороненої інформації, можливо прогнозування процесу її поширення.

Висновки. Підсумовуючи проведений аналіз наукової літератури можна засвідчити недостатню кількість досліджень, які стосуються даної проблеми. Описано комп'ютерні мережі, що знаходяться під впливом загрози поширення забороненої інформації, також проведено аналіз проблем інформаційної безпеки. Створення моделей і алгоритмів поширення загрози забороненої інформації - один з ключових підходів при вирішенні проблеми забороненого контенту. При моделюванні ЗгЗІ важливо мати топологію, яка відображатиме структуру зв'язків реальної мережі, а також використовувати адекватну модель інформаційної взаємодії вузлів. Ще однією важливою проблемою є великомасштабність КМ, яка заважає отримати дані з імітаційної моделі за прийнятний час. Вирішення цього завдання полягає в створенні аналітичної моделі ЗгЗІ в КМ. Думаю після того як провести інформаційний огляд і експерименти для виявлення істотних характеристик об'єкта і зовнішніх факторів, що впливають на процес реалізації ЗгЗІ, виконати аналіз основних підходів до моделювання ЗгЗІ, розробити імітаційну модель ЗгЗІ в КМ, синтезувати і показати адекватність аналітичної моделі ЗгЗІ в КМ, розробити методику формування топології КМ, змоделювати процес реалізації ЗгЗІ на топології реальної великомасштабної КМ і провести експериментальне дослідження з отриманими результатами, буде можливим підвищення точності прогнозування загрози поширення забороненої інформації в комп'ютерних мережах.

ЛІТЕРАТУРА:

1. Губанов Д.А. Соціальні мережі: моделі інформаційного впливу, керування і протистояння / Д.А. Губанов, Д.А. Новиков, А.Г. Чхартишвили; под. ред. чл..-корр. РАН Д.А. Новикова – М.: Видав. Фізико-математичної літератури, 2010. – 228 с.

2. Albert R. Statistical mechanics of complex networks / R. Albert, A. Barabasi; Rewiews of Modern Physics, 2002.

3. Easley D. Networks, Crowds and Markets Reasoning About a Highly Connected World / D. Easley, J. Kleinberg, 2010.

4. Chwe M.S. Communication and Coordination in Social Network / M.S. Chwe; Review of Economic Studies, 2000.

5. Ferrara E. Topological features of Online Social Networks. Communications on Applied and Industrial Mathematics / E. Ferrara, G. Fiumara, 2011.

6. Закон України про захист суспільної моралі [Електронний ресурс] – Режим доступу: http://zakon2.rada.gov.ua/laws/show/1296-15

REFERENCES:

1. Hubanov D.A. Sotsialni merezhi: modeli informatsiinoho vplyvu, keruvannia i protystoiannia / D.A. Hubanov, D.A. Novykov, A.H. Chkhartyshvyly; pod. red. chl..-korr. RAN D.A. Novykova – M.: Vydav. Fizyko-matematychnoi literatury, 2010. – 228 s.

2. Albert R. Statistical mechanics of complex networks / R. Albert, A. Barabasi; Rewiews of Modern Physics, 2002.

3. Easley D. Networks, Crowds and Markets Reasoning About a Highly Connected World / D. Easley, J. Kleinberg, 2010.

4. Chwe M.S. Communication and Coordination in Social Network / M.S. Chwe; Review of Economic Studies, 2000.

5. Ferrara E. Topological features of Online Social Networks. Communications on Applied and Industrial Mathematics / E. Ferrara, G. Fiumara, 2011.

6. Zakon Ukrainy pro zakhyst suspilnoi morali [Elektronnyi resurs] – Rezhym dostupu: http://zakon2.rada.gov.ua/laws/show/1296-15.

Без рецензії.

к.т.н. Бойчук В.О., Юмашов В.С.

МЕТОД ОБНАРУЖЕНИЯ УГРОЗЫ РАСПОСТРАНЕНИЯ ЗАПРЕЩЕННОЙ К ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

В статье рассматриваются компьютерные сети (КС), которые находяться под влиянием угрозы распространения запрещенной информации. Исследуются модели угрозы распространения этой информации и особенности компьютерных сетей. Приведены основные проблемы информационной безопасности, которые актуальны для даного исследования и алгоритм по котрому осуществляется функцыонирование компьютерных сетей, находящихся под влиянием угрозы распостранения запрещенной информации. С бурным ростом числа пользователей КМ возникают проблемы информацыонной безопасности и защиты информации в них. Анализ етих проблем обнаружил, что существует малоизученная проблема запрещенного контента. Создание моделей и алгоритмов распостранения угрозы запрещенной информации – один из ключевых подходов при решении даной задачи.

Ключевые слова: безопасность компютерных сетей, запрещенная информация, большое количество пользователей, моделирования.

Ph.D. Boychuk V.O., Yumashov V.S.

METHOD FOR DETECTION OF THREATS DISTRIBUTE ILLEGAL TO SPREAD INFORMATION IN COMPUTER NETWORKS

The article deals with computer networks, which are influenced by the threat of banned information. Investigate the threat model disseminate this information and especially computer networks. The basic problem of information security, which are relevant for research and danogo MDM algorithm implemented funktsyonirovanie computer networks, which are under threat proliferation forbidden information. With the rapid increase in the number of users of computer networks problems informatsyonnoy safety and protection of the information in them. Analysis etih problems found that there raises the problem of inappropriate content. Creating models and the proliferation threat information gap algorithms - one of the key approaches to addressing this problem.

Keywords: security computer networks, prohibited information, a large number of users, modeling.