ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004.891

д.т.н., проф. **Лєнков С.В.** (ВІКНУ)
к.т.н., доц. **Джулій В.М.** (ХмНУ)
д.т.н., с.н.с. **Сєлюков О.В.** («Укрспецконсалтинг»)
к.т.н., доц. **Орленко В.С.** (ХмНУ)
Атаманюк А.В. (ХмКК ХКТЕ)

DOI: https://doi.org/10.17721/2519-481X/2020/68-06

МОДЕЛЬ БЕЗПЕКИ ПОШИРЕННЯ ЗАБОРОНЕНОЇ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

У статті запропоновано підхід до визначення моделі безпеки поширення забороненої інформації в інформаційно-телекомунікаційних мережах.

Найбільш ефективне прогнозування поширення загрози забороненої інформації здійснюється за допомогою моделювання даного процесу. Інформаційно-телекомунікаційні мережі є великомасштабними мережами з постійно зростаючим числом абонентів. З бурхливим зростанням кількості користувачів ІТКМ виникають проблеми інформаційної безпеки і захисту інформації в них. Проведений аналіз проблем інформаційної безпеки виявив, що крім проблем, пов'язаних з використанням глобальної мережі Інтернет як розподіленої інформаційно-телекомунікаційної системи, які досить добре відомі і можна вирішити, існує маловивчена проблема забороненого контенту.

Створення моделей і алгоритмів поширення загрози забороненої інформації – один з ключових підходів при вирішенні даної задачі. Проведений аналіз публікацій з даної тематики показує, що існуючі рішення малоефективні. Зазвичай при моделюванні поширення загрози забороненої інформації не враховується топологія ІТКМ (модель мережі – повнозв'язний граф). При моделюванні загрози поширення забороненої інформації важливо мати топологію, яка відображатиме структуру зв'язків реальної мережі, а також використовувати адекватну модель інформаційної взаємодії вузлів. Ще однією важливою проблемою є великомасштабність ІТКМ, яка заважає отримати дані з імітаційної моделі за прийнятний час. Розв'язання цієї задачі полягає у створенні аналітичної моделі загрози поширення забороненої інформації в ІТКМ.

Розроблено алгоритм реалізації ЗПЗІ (загрози поширення забороненої інформації) в ІТКМ, заснований на характерах процесів, що протікають в реальних умовах.

Запропонована імітаційна модель ЗПЗІ в ІТКМ, яка враховує топологічні характеристики мережі, а також особливості інформаційної взаємодії абонентів як людино-машинних систем. З її допомогою проведені експерименти, результати яких показали залежність реалізації ЗПЗІ від топологічної уразливості мережі. Розроблено аналітичну модель ЗПЗІ з урахуванням топологічної уразливості мережі. Релевантність результатів аналітичного рішення підтверджена серією експериментів на топології реальної мережі з використанням імітаційного моделювання. При цьому похибка для процесу захисту склала не більше 10%, для процесу атаки – не більше 15%.

Ключові слова: інформаційна безпека, аналітична модель, імітаційна модель, поширення загроз, інформаційна взаємодія, модель мережі.

Вступ. Інформаційно-телекомунікаційні мережі (ІТКМ) забезпечують практично повний спектр можливостей для обміну інформацією між користувачами – мережевими абонентами. Сучасною проблемою таких систем є їх низький рівень інформаційної безпеки. Ефективного захисту абонентів від загрози поширення забороненої інформації, зокрема в умовах широкого використання індивідуально-орієнтованих сервісів і пов'язаних з ними протоколів і технологій (SOAP, CORBA, REST тощо), не існує. Серед безлічі функцій захисту принциповою в відношенні даних систем є функція попередження прояву забороненої інформації. Вона реалізується за рахунок механізмів прогнозування загрози поширення і

розсилання повідомлень з попередженнями про наслідки дій зі забороненим контентом. Використання інших функцій (попередження, виявлення, локалізації та ліквідації загрози) припускає наявність повного контролю над системою, що в реальних умовах неможливо.

Інформаційно-телекомунікаційна мережа надає різні сервіси для організації соціальних взаємовідносин між користувачами (абонентами). На сьогоднішній день найбільш популярними з них є соціальні мережі. З бурхливим ростом кількості користувачів інформаційно-телекомунікаційних мереж виникають і проблеми безпеки в них. Узагальнена структурна схема інформаційно-телекомунікаційних мереж (ІТКМ) приведена на рис. 1. Її склад в загальному випадку утворюють такі функціональні елементи:

- абоненти (А). Під абонентом розуміється людино-машинна система, що складається з пристрою, через який здійснюється доступ до мережі, і безпосередньо користувача ІТКМ. Абоненти можуть бути окремими вузлами мережі (якщо користувач використовує свій домашній комп'ютер), або можуть бути об'єднані в корпоративну обчислювальну мережу (КОМ) (якщо абонент використовує робочий комп'ютер), 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 тощо), для доступу до мережі. Також використовують програмне забезпечення (спеціальний додаток) і модулі захисту (МЗ);

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

- КОМ містить 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 абонентів між собою;

- керуючий елемент технічно є сукупністю 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 тощо).

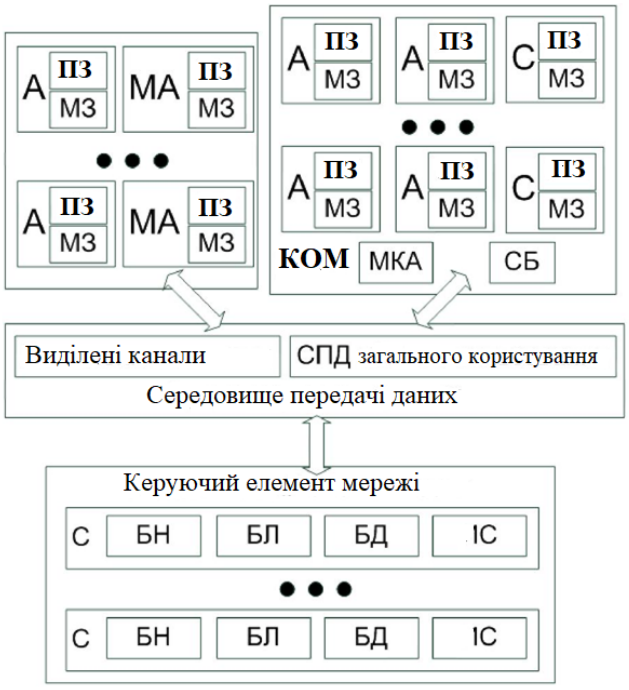

Рисунок 1 – Структурна схема ІТКМ

Розглянемо існуючі проблеми інформаційної безпеки в інформаційно-телекомунікаційних мережах, які актуальні для даного дослідження:

1. Використання глобальної мережі Інтернет як розподіленої інформаційно-телекомунікаційної системи. Найбільш вразливими компонентами системи, що часто атакуються, є: сервери; робочі станції; середовище передачі інформації; вузли комутації. Типові інформаційні впливи зловмисників:

Прослуховування мережевого трафіку. Щоб прослухати трафік (sniffing) мережевий адаптер переводиться в «безладний» режим. У цьому режимі адаптер перехоплює всі мережеві пакети, що проходять через нього, а не тільки призначені даною адресою, 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 EYE і TCP Dump.

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

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

Сканування вразливостей. Результатом роботи сканера є інформація про систему, що містить список мережевого обладнання, комп'ютерів з запущеними на них службами, версіями мережевого ПЗ (а отже і вразливостей, властивих даному ПЗ), облікові записи користувачів. Сканування вразливостей зазвичай є етапом, що передує атаку. Саме результати сканування дозволяють точно підібрати експлойти для здійснення безпосереднього НСД.

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 кроки сканування можна, вивчаючи журнали реєстрації міжмережевих екранів (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 здійснювати 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.

Мережеві атаки. Мережеві атаки можна розділити на: атаки, засновані на переповненні буфера (overflow based attacks). Вони використовують вразливість системи, яка полягає в некоректній програмної обробці даних. При цьому з'являється можливість виконання шкідливого коду з підвищеними привілеями; 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, що їй посилають, призводять до значної витрати ресурсів системи. Найпростішим прикладом атаки цього типу є атака «Ping Of Death». Суть її в наступному: на комп'ютер жертви надсилається сильно фрагментований ICMP-пакет великого розміру. Реакцією ОС Windows на отримання такого пакету є повне зависання.

Атаки, засновані на використанні вразливостей в ПЗ мережевих додатків – експлойти (exploit). Даний клас атак заснований на експлуатації різних дефектів в ПЗ. Експлойти є шкідливими програмами, що реалізують відому вразливість в ОС або прикладному ПЗ, для отримання НСД до вразливого хосту або порушення його працездатності. Для експлойтів характерна наявність функцій подавлення антивірусних програм і МЕ. Наслідки застосування

експлойтів можуть бути самими критичними. У випадку отримання зловмисником віддаленого доступу до системи, він має практично повний (системний) доступ до комп'ютера. Наступні дії і збиток від них можуть бути такими: впровадження троянської програми, впровадження набору утиліт для приховування факту компрометації системи, несанкціоноване копіювання зловмисником даних з жорстких та зовнішніх носіїв інформації, створення на віддаленому комп'ютері нових облікових записів з будь-якими правами в системі для подальшого доступу як віддалено, так і локально, крадіжка файлів з хешами паролів користувачів, знищення або модифікація інформації, здійснення дій від імені користувача системи.

Протидія. МЕ і СОВ, встановлені на системі, що атакується, в деяких випадків не в змозі відобразити дію експлойтів. Для успішного відображення атак експлойтів засоби захисту необхідно оновлювати, оскільки механізм виявлення вторгнень заснований на розпізнаванні сигнатур вже відомих атак. Хоча є розробки, здатні за завіреннями розробників відображати невідомі атаки, практика показує, що вони все ще не ефективні.

Шкідливі програми. Шкідливі програми – це комп'ютерна програма або переносний код, призначений для реалізації загроз інформації, що зберігається в мережі, або для прихованого нецільового використання ресурсів або якого іншого впливу, що перешкоджає нормальному функціонуванню мережі. До шкідливих програми відносяться комп'ютерні віруси, троянські коні, мережеві черв'яки тощо.

Протидія. Типовим методом протидії є застосування 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, описи насильства, в тому числі сексуального, екстремізм і розпалювання расової ненависті. В українському законодавстві кілька законів регулюють питання надання інформації про фізичних та юридичних осіб, а саме: Закон України «Про інформацію» від 02.10.92, що регулює відносини щодо одержання і поширення інформації; Закон України «Про захист персональних даних» від 01.06.2010, що визначає захист і обробку персональних даних; Закон України «Про доступ до публічної інформації» від 13.01.2011, який надає право на отримання інформації, що знаходиться у володінні розпорядників.

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, що регулярно здійснюються в автоматизованих системах різними засобами і методами з метою створення, підтримки і забезпечення умов, об'єктивно необхідних для надійного захисту інформації.

Перелік повної множини 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 незадовільна, а в інтернет-просторі загострюється через технічні складнощі.

2. Попередження безпосередньої прояви забороненої інформації. Функція реалізується за рахунок механізмів прогнозування поширення забороненої інформації в соціальній мережі.

3. Виявлення забороненої інформації, яка проявилася. Функція пов'язана з моніторингом ІТКМ на предмет забороненої інформації на сторінках абонентів. Як правило, для реалізації даного захисту використовується різні СОРМ (система оперативно-розшукових заходів). 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 автоматичного пересилання повідомлення з попередженням про відповідальність за розповсюдження забороненої інформації, аж до блокування абонента. Блокування може здійснюватися легітимними засобами за наявності доступу до керування системи та нелегітимними – при його відсутності (зламання акаунта). ФЗ ділиться на дві функції. Перша пов'язана з попередженням абонентів, на сторінках яких була знайдена заборонена інформація, а друга – з розсилкою попереджень потенційним одержувачам 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.

6. Локалізація, обмеження впливу забороненої інформації на абонентів. Функція реалізується через блокування абонентів, що поширюють заборонену інформацію, або абонентів – потенційних розповсюджувачів. Дана ФЗ опирається 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 основі проведеного аналізу функцій захисту видно, що найбільш ефективні функції – це перші функції, оскільки вони забезпечують захист на початкових етапах. Наведені функції захисту мають свої недоліки. Найбільш перспективною ФЗ інженерно-технічного напряму є $ФЗ_2$. На даному етапі, маючи інформацію про топології ІТКМ і потенційних розповсюджувачів забороненої інформації, можливе прогнозування процесу її поширення.

Постановка задачі. Одним з підходів до прогнозування загрози поширення забороненої інформації (ЗПЗІ) є моделювання, наприклад, з використанням моделей впливу, моделей просочування і зараження. Дані моделі, як правило, не враховують топологічні особливості мережі (розподіл ступенів зв'язності, кластерний коефіцієнт, середня довжина шляху). Взаємодія між абонентами в межах цих математичних моделей описується переважно гомогенним графом, що при моделюванні великомасштабних мереж (більше 10 млн. вузлів) може дати похибку прогнозування загрози поширення забороненої інформації більше 30%. Крім того, дані підходи мають в основному теоретичний характер, практика їх використання не виходить за межі експериментів. Таким чином, дослідження, спрямовані на створення моделей та алгоритмів загрози поширення забороненої інформації, актуальні і мають теоретичне і практичне значення у вирішенні проблеми забезпечення інформаційної безпеки в системах і мережах телекомунікацій.

Створення моделей та алгоритмів поширення загрози забороненої інформації – одна з ключових задач в даному напрямку. При її вирішенні виникають проблеми, пов'язані з властивостями розглянутої інформаційно-телекомунікаційної системи, а саме:

1. Відсутність перевірки достовірності даних про вузол системи. Дуже часто абоненти ІТКМ вказують недостовірну інформацію про себе.

2. Закритість системи. Структура та інформація про управління системою є конфіденційною інформацією.

3. Проблема збору інформації. Неможливо отримати повну інформацію про топологію ІТКМ. Існує можливість для звичайного абонента збору інформації про структуру мережі (функції API), але ця можливість має багато обмежень (налаштування приватності, часовий інтервал).

Найбільш ефективне прогнозування поширення загрози забороненої інформації здійснюється за допомогою моделювання даного процесу.

Прведений аналіз проблем інформаційної безпеки виявив, що крім проблем, пов'язаних з використанням глобальної мережі Інтернет як розподіленої інформаційно-телекомунікаційної системи, які досить добре відомі і можна вирішити, існує маловивчена проблема забороненого контенту, існуючі рішення малоефективні.

Зазвичай при моделюванні поширення загрози забороненої інформації не враховується топологія ІТКМ (модель мережі – повнозв'язний граф). А, якщо топологія враховується, то, як правило, використовується найпростіша SIS модель, а структура мережі відбивається SF мережею. При моделюванні загрози поширення забороненої інформації важливо мати топологію, яка відображатиме структуру зв'язків реальної мережі, а також використовувати адекватну модель інформаційної взаємодії вузлів. Ще однією важливою проблемою є великомасштабність ІТКМ, яка заважає отримати дані з імітаційної моделі за прийнятний час. Розв'язання цієї задачі полягає у створенні аналітичної моделі загрози поширення забороненої інформації в ІТКМ.

Основна частина. За результатами проведеного дослідження предметної області вставлено необхідність розробки імітаційної і аналітичної моделей поширення загрози забороненої інформації в ІТКМ. Імітаційна модель необхідна для отримання експериментальних результатів для синтезування аналітичної моделі. Необхідність створення аналітичної моделі обґрунтовується тим, що для імітаційного моделювання на топології існуючих ІТКМ (десятки мільйонів вузлів) необхідні великі витрати часу. Не враховуючи час на збір інформації про топології мережі, який може становити близько тижня, безпосередньо моделювання загрози поширення забороненої інформації (ЗПЗІ) займає кілька годин навіть при використанні розподілених обчислювальних ресурсів. Аналітична модель може дати прогноз загрозі поширення забороненої інформації майже миттєво. З її допомогою можна отримати актуальні дані (до того моменту, коли кількість атакуючих абонентів буде максимальним) за динамікою ЗПЗІ.

Процес ЗПЗІ характеризується наступними особливостями. У мережі існують вузли трьох типів. Перший тип – атакуючі вузли, це вузли, які розповсюджують заборонену інформацію. Другий тип – захищені вузли, які характеризуються тим, що не беруть участі в поширенні забороненої інформації і ніколи не будуть цим займатися. Третій тип – потенційно вразливі. Вузли такого типу не беруть участі в процесі поширення загрози, але можуть бути схильні до негативного впливу з боку атакуючих вузлів і можуть почати поширювати заборонену інформацію.

Аналітична модель динаміки атаки $I(t)$ та модель ахисту вузлів $R(t)$ представлені наступним чином (1):

$$\begin{cases} I(t) = f(N, \beta, \gamma, \varphi, t) \\ R(t) = g(N, \beta, \gamma, \varphi, t) \end{cases} \quad (1)$$

де, N – кількість вузлів, яка дорівнює кількості абонентів мережі, β – параметр, що відображає силу загрози, ймовірність здійснення атаки, γ – параметр, що відображає ступінь протидії загрозі, ймовірність захисту абонента (β і γ в даному дослідженні визначено як константи, але можуть бути виражені як функції, що залежать від психосемантичних профілів абонентів ІТКМ), φ – коефіцієнт топологічної вразливості мережі, що відображає внутрішню властивість ІТКМ, засновану на характеристиках її топології, яке сприяє поширенню забороненої інформації , t – час процесу (в умовних одиницях часу).

Розробка аналітичної моделі включає в себе послідовність наступних дій:

- формування імітаційної моделі для дослідження характеру і параметрів процесу ЗПЗІ;
- синтез аналітичних залежностей параметрів процесу;
- проведення експериментів з метою перевірки точності (адекватності) моделі.

Наведемо алгоритм реалізації ЗПЗІ, грунтуючись на описі процесів, що відбуваються в реальних ІТКМ. Схема реалізації загрози зображена на рис. 2.

Алгоритм загрози поширення забороненої інформації в ІТКМ

1. Поширення забороненої інформації (ЗІ) (далі процес «атаки») ініціює будь-який абонент-зловмисник (на рис. 2 – вузол 1), поширюючи повідомлення з ЗІ (реалізує загрозу) за його списком контактів. Атаку може починати один зловмисник або група.

2. Абоненти-одержувачі (вузли 2, 3, 4), прийнявши повідомлення з ЗІ, читають його і включаються в процес атаки, поширюючи її далі по своєму списку контактів (вузол 3), або ігнорують або взагалі видаляють повідомлення (вузол 2) , 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 тощо.

3. Абоненти можуть перестати сприймати і, відповідно, поширювати ЗІ (вузол 5) (далі процес «захисту»), внаслідок впливу механізмів захисту (наприклад, попередження про неї), тому повідомлення з ЗІ від атакуючих абонентів будуть постійно відхилятися.

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

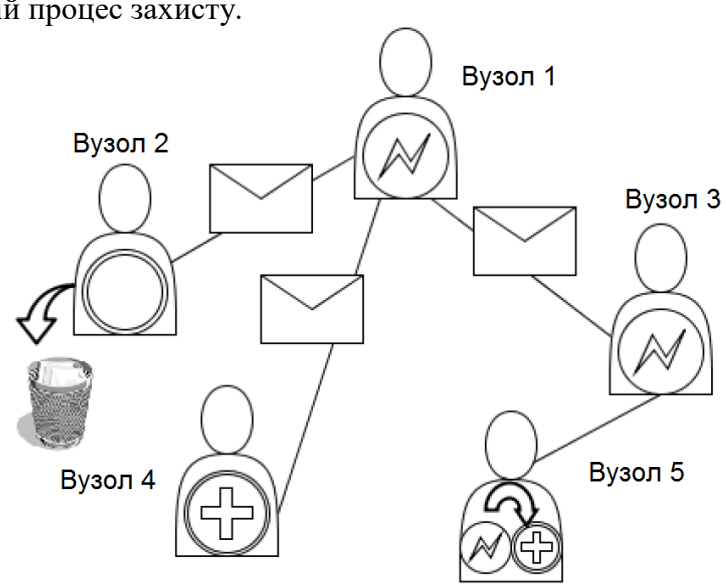

Рисунок 2 – Схема реалізації загрози поширення забороненої інформації в ІТКМ

Таким чином, ЗПЗІ в ІТКМ є складним динамічним процесом, що складається з двох протидіючих підпроцесів атаки і захисту вузлів мережі.

На основі описаного алгоритму побудована імітаційна модель ЗПЗІ в ІТКМ:

Вхідні дані: N, k – середній ступінь зв'язності вузлів, a – параметр, що відображає середню довжину шляху і рівень мережевої кластеризації, β, γ (в моделі вважається, що β та γ однакові для кожного абонента), I_0 - кількість абонентів-зловмисників - початкових джерел загроз, R_0 - кількість абонентів спочатку несприйнятливих до атакуючих дій.

Вихідні дані: $I(t), R(t), S(t)$ – чисельні масиви даних, що описують динамічний процес реалізації ЗПЗІ (кількості атакуючих, захищених і потенційно вразливих вузлів у кожну умовну одиницю часу відповідно).

1. Створення топології ІТКМ – графа $G_{SW} = \langle V, E \rangle$, де G_{SW} – граф small-world мережі (на основі моделі Watts-Strogatz), $V = \{v_i\}$ – множина вершин, $E = \{e_{ij}\}$ – множина ребер, $i = \overline{1, N}$, $j = \overline{1, N}$. Даний крок здійснюється з використанням програми Pajek, адаптованої під цю задачу, за рахунок заданих топологічних параметрів *N, k, a*.

2. Сформувати множину $V = \{V^I, V^S, V^R\}$, де $V^I = \{v_i^I\}$ – множина атакуючих вузлів $\left(\left|V^I\right| = I_0\right)$, $V^R = \{v_i^R\}$ – множина захищених вузлів $\left(\left|V^R\right| = R_0\right)$, $V^S = \{v_i^S\}$ – множина потенційно вразливих вузлів $\left(\left|V^S\right| = N - I_0 - R_0\right)$.

3. $\forall v_i^I$, якщо $\exists e_{ij}$ та $v_j \in V^S$, $j = \overline{1,N}$, то з ймовірністю β виконати: $V^S \setminus v_j$ та $V^I \bigcup v_j$; з ймовірністю γ виконати: $V^I \setminus v_i, V^R \bigcup v_i$.

4. Якщо $V^I = \varnothing$ або $\gamma = 0$ та $V^S = \varnothing$, то кінець алгоритму, інакше перейти до п. 3.

Аналізуючи процес інформаційної взаємодії абонентів при поширенні забороненої інформації в ІТКМ, можна зробити наступні висновки. Маємо справу з трьома типами абонентів: атакуючі абоненти, які поширюють заборонену інформацію, захищені абоненти, які характеризуються тим, що не беруть участі в поширенні забороненої інформації і ніколи не будуть цим займатися, і потенційно вразливі абоненти, які можуть бути схильні до негативного впливу з боку атакуючих вузлів і можуть почати поширювати заборонену інформацію. При цьому ми спостерігаємо два протиборчих підпроцеси атаки і захисту абонентів мережі. Для моделювання таких явищ часто застосовують епідеміологічні моделі , зокрема нашому опису відповідає SIR-модель Кермак-Маккендріка. Характер графіків, отриманих у результаті імітаційного моделювання (рис. 3), подібний з результатами, що дає дана модель. Виходячи з вищесказаного, приходимо до висновку, що дана модель є найбільш релевантною для цього дослідження

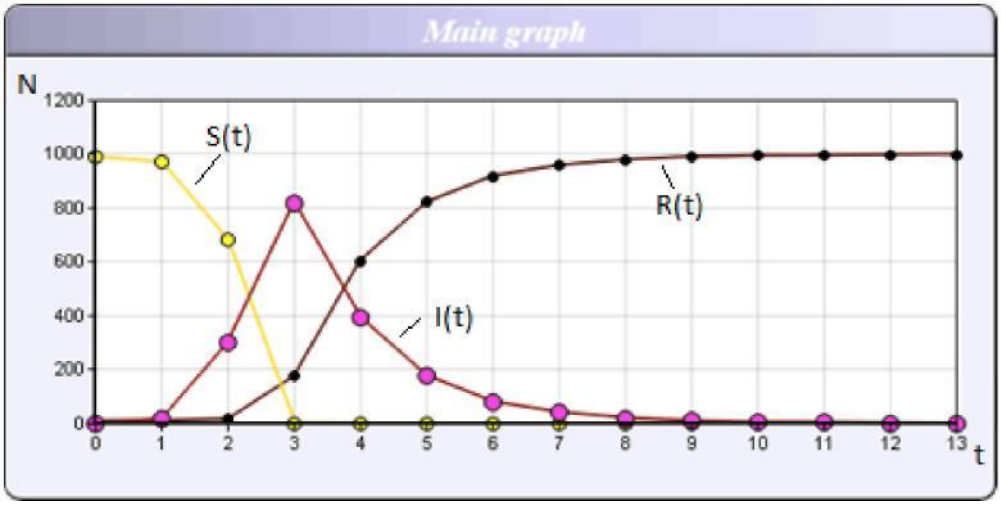

Рисунок 3 – Імітаційне моделювання
($N = 1000$, $\varphi = 20$, $I_0 = 1$, $\beta = 0.5$, $\gamma = 0.5$, $R_0 = 10$), $S(t)$ – кількість схильних до атаки вузлів

SIR–епідеміологічна модель, що спрощено описує поширення захворювання, які передаються від одного індивіда до іншого, яка розглядає суб'єктів з точки зору трьох можливих станів: сприйнятливий, інфікований, імунізований.

Система диференціальних рівнянь, що описують SIR-модель, має вигляд:

$$\begin{cases} \dfrac{\partial I}{\partial t} = \beta \cdot \dfrac{S(t) \cdot I(t)}{N} - \gamma \cdot I(t) \\ \dfrac{\partial R}{\partial t} = \gamma \cdot I(t) \\ \dfrac{\partial S}{\partial t} = -\beta \cdot \dfrac{S(t) \cdot I(t)}{N} \end{cases} \quad (2)$$

де, $I(t)$ – кількість заражених (інфікованих) особин, $S(t)$ – кількість сприятливих особин, $R(t)$ – кількість «виключених з імунізацією» особин, $N = I(t) + S(t) + R(t)$ – кількість особин у популяції, γ – коефіцієнт відновлення / смерті, β – коефіцієнт зараження (інфікування), t – час.

При використанні системи (2) для аналізу ЗПЗІ в ІТКМ отримуємо результати, які хоча і адекватно описують характер процесу, але не дають потрібної точності прогнозу.

На основі проведенго аналізу даних, отриманих за результатами імітаційного моделювання та аналітичного рішення системи (2), і простеживши фізичний зміст рівнянь в даній системі, можна прийти до наступного висновку: процес атаки залежить від структури зв'язків між абонентами в мережі. Параметр топологічної вразливості φ може впливати на $I(t)$ через коефіцієнт β. У загальному вигляді адаптовану систему (2) можна представити в наступному вигляді

$$\begin{cases} \dfrac{\partial I}{\partial t} = 2 \cdot \ln \varphi \cdot \beta \cdot \dfrac{S(t) \cdot I(t)}{N} - \gamma \cdot I(t) \\ \dfrac{\partial R}{\partial t} = \gamma \cdot I(t) \\ \dfrac{\partial S}{\partial t} = -2 \cdot \ln \varphi \cdot \beta \cdot \dfrac{S(t) \cdot I(t)}{N} \end{cases} \quad (3)$$

Система диференціальних рівнянь (3) дозволяє отримати прогноз ЗПЗІ у великомасштабної ІТКМ ($N = 10^5..10^8$) з похибкою до 18%.

Висновки. Інформаційно-телекомунікаційні мережі є великомасштабними мережами з постійно зростаючим числом абонентів. З бурхливим зростанням кількості користувачів ІТКМ виникають проблеми інформаційної безпеки і захисту інформації в них.

Аналіз проблем інформаційної безпеки виявив, що крім проблем, пов'язаних з використанням глобальної мережі Інтернет як розподіленої інформаційно-телекомунікаційної системи, які досить добре відомі і можна вирішити, існує маловивчена проблема забороненого контенту.

Створення моделей і алгоритмів поширення загрози забороненої інформації – один з ключових підходів при вирішенні даної задачі. Проведений аналіз публікацій з даної тематики показує, що існуючі рішення малоефективні. Зазвичай при моделюванні поширення загрози забороненої інформації не враховується топологія ІТКМ (модель мережі – повнозв'язний граф). А, якщо топологія враховується, то, як правило, використовується найпростіша SIS модель, а структура мережі відбивається SF мережею. При моделюванні загрози поширення забороненої інформації важливо мати топологію, яка відображатиме структуру зв'язків реальної мережі, а також використовувати адекватну модель інформаційної взаємодії вузлів. Ще однією важливою проблемою є великомасштабність ІТКМ, яка заважає отримати дані з імітаційної моделі за прийнятний час. Розв'язання цієї задачі полягає у створенні аналітичної моделі загрози поширення забороненої інформації в ІТКМ.

Розроблено алгоритм реалізації ЗПЗІ в ІТКМ, заснований на характерах процесів, що протікають в реальних умовах.

Запропонована імітаційна модель ЗПЗІ в ІТКМ, що враховує топологічні характеристики мережі, а також особливості інформаційної взаємодії абонентів як людино-машинних систем. З її допомогою проведені експерименти, результати яких показали залежність реалізації ЗПЗІ від топологічної уразливості мережі.

Розроблено аналітичну модель ЗПЗІ з урахуванням топологічної уразливості мережі. Релевантність результатів аналітичного рішення підтверджена серією експериментів на топології реальної мережі з використанням імітаційного моделювання. При цьому похибка для процесу захисту склала не більше 10%, для процесу атаки – не більше 15%.

ЛІТЕРАТУРА:

1. Кримінальний кодекс України від 05.04.2001 № 2341-III. Дата оновлення: 25.09.2020. URL: http://zakon2.rada.gov.ua/laws/show/2341-14/page (дата звернення: 02.09.2020).

2. Про інформацію: Закон України від 02.10.1992 №2657-XII. Дата оновлення: 16.07.2020. URL: http://zakon2.rada.gov.ua/laws/main/2657-12 (дата звернення: 02.09.2020).

3. Про науково-технічну інформацію: Закон України від 25.06.1993 № 3322-XII. Дата оновлення: 19.04.2014. URL: http://zakon5.rada.gov.ua/laws/main/3322-12 (дата звернення: 02.09.2020).

4. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. Дата оновлення: 04.07.2020. URL: http://zakon5.rada.gov.ua/laws/show/80/94-вр (дата звернення: 02.09.2020).

5. Про електронні довірчі послуги: Закон України від 05.10.2017 № 2155-VIII. Дата оновлення: 13.02.2020. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 02.09.2020).

6. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. Дата оновлення: 20.03.2020. URL: http://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 02.09.2020).

7. Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI. Дата оновлення: 01.10.2020. URL: https://zakon.rada.gov.ua/laws/show/2939-17 (дата звернення: 02.09.2020).

8. Концепція розвитку системи електронних послуг в Україні. Розпорядження Кабінету Міністрів України від 16.11.2016 р. № 918-р. URL: http://zakon3.rada.gov.ua/laws/show/918-2016-%D1%80 (дата звернення: 02.09.2020).

9. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури. Постанова Кабінету Міністрів України від 19 червня 2019 року № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (дата звернення: 02.09.2020).

10. Аналізатор Sniffer Pro LAN. URL: https://www.securitylab.ru/software/233623.php (дата звернення: 02.09.2020).

11. Аналіз та візуалізація дуже великих мереж. URL: http://mrvar.fdv.uni-lj.si/pajek/ (дата звернення: 02.09.2020).

12. Биячуев, Т.А. Безопасность корпоративных сетей: учеб. пособие / Т.А. Биячуев; под ред. Осовецкого Л.Г. – СПб.: СПбГУ ИТМО, 2016. – 161 с.

13. Брэгг, Р., Родс-Оусли, М., Страссберг, К. Безопасность сетей. Полное руководство / Р. Брэгг, М. Родс-Оусли, К. Страссберг; – М : Эком, 2006. – 912 с.

14. Завдада А.А. Аналіз сучасних систем виявлення атак і запобігання вторгненням / А.А. Завада, О.В. Самчишин, В.В. Охрімчук // Збірник наукових праць ЖВІ НАУ «Інформаційні системи'12», 2012. – Випуск 6. – С. 97 – 106.

15. Загальні рекомендації щодо підвищення рівня захищеності інформаційних ресурсів при віддаленій роботі співробітників установи. URL:

http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article;jsessionid=322B14F318F82FDEB1180D17FE0BFF97.app1?showHidden=1&art_id=320060&cat_id=317163 (дата звернення: 02.09.2020).

16. Kolotov, A. Мониторинг сети с помощью tcpdump. URL: http://www.linuxshare.ru/docs/net/tcpdump.html (дата звернення: 02.09.2020).

17. Лукацький, А.В. Предотвращение сетевых атак: технологии и решения / А.В. Лукацкий. – СПб. : Экспрес Электроника, 2006. – 268 с.

18. Столлингс, В. Основы защиты сетей. Приложения и стандарты / В. Столлингс. – М.: Издательский дом "Вильямс", 2002. – 432 с.

19. Тропіна М. Дослідження соціальних мереж як нового феномену сучасного світу / М. Тропіна // Наукові записки Малої академії наук України. Серія «Педагогічні науки» : [зб. наук. праць; редкол. : С.О. Довгий (голова), О.Є. Стрижак, О.В. Лісовий, І.М. Савченко та ін.]. – Київ : Національний центр «Мала академія наук України», 2019. – Вип. 16. – С. 57-63 (76 с.)

REFERENCES:

1. Kryminal′nyy kodeks Ukrayiny vid [The Crimean Code of Ukraine from] 05.04.2001 № 2341-III. Data onovlennya: 25.09.2020. URL: http://zakon2.rada.gov.ua/laws/show/2341-14/page (data zvernennya: 02.09.2020).

2. Pro informatsiyu : Zakon Ukrayiny vid [About information : Law of Ukraine from] 02.10.1992 №2657-XII. Data onovlennya: 16.07.2020. URL: http://zakon2.rada.gov.ua/laws/main/2657-12 (data zvernennya: 02.09.2020).

3. Pro naukovo-tekhnichnu informatsiyu : Zakon Ukrayiny vid [About scientific and technical information : Law of Ukraine from] 25.06.1993 № 3322-XII. Data onovlennya: 19.04.2014. URL: http://zakon5.rada.gov.ua/laws/main/3322-12 (data zvernennya: 02.09.2020).

4. Pro zakhyst informatsiyi v informatsiyno-telekomunikatsiynykh systemakh : Zakon Ukrayiny vid [On information protection in information and telecommunication systems : Law of Ukraine from] 05.07.1994 № 80/94-VR. Data onovlennya: 04.07.2020. URL: http://zakon5.rada.gov.ua/laws/show/80/94-вр (data zvernennya: 02.09.2020).

5. Pro elektronni dovirchi posluhy : Zakon Ukrayiny vid [About electronic trust services : Law of Ukraine from] 05.10.2017 № 2155-VIII. Data onovlennya: 13.02.2020. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (data zvernennya: 02.09.2020).
6. Pro zakhyst personal′nykh danykh : Zakon Ukrayiny vid [On personal data protection : Law of Ukraine from] 01.06.2010 № 2297-VI. Data onovlennya: 20.03.2020. URL: http://zakon.rada.gov.ua/laws/show/2297-17 (data zvernennya: 02.09.2020).
7. Pro dostup do publichnoyi informatsiyi : Zakon Ukrayiny vid [On access to public information : Law of Ukraine from 13.01.2011] 13.01.2011 № 2939-VI. Data onovlennya: 01.10.2020. URL: https://zakon.rada.gov.ua/laws/show/2939-17 (data zvernennya: 02.09.2020).
8. Kontseptsiya rozvytku systemy elektronnykh posluh v Ukrayini. Rozporyadzhennya Kabinetu Ministriv Ukrayiny vid [The concept of development of the electronic services system in Ukraine. Order of the Cabinet of Ministers of Ukraine from] 16.11.2016 p. № 918-p. URL: http://zakon3.rada.gov.ua/laws/show/918-2016-%D1%80 (data zvernennya: 02.09.2020).
9. Pro zatverdzhennya Zahal′nykh vymoh do kiberzakhystu ob″yektiv krytychnoyi infrastruktury. Postanova Kabinetu Ministriv Ukrayiny vid [On approval of the General requirements for cyber protection of critical infrastructure. Resolution of the Cabinet of Ministers of Ukraine of June 19, 2019] 19.06.2019 № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (data zvernennya: 02.09.2020).
10. Analizator Sniffer Pro LAN. URL: https://www.securitylab.ru/software/233623.php (data zvernennya: ата звернення: 02.09.2020).
11. Analysis and visualization of very large networks. URL: http://mrvar.fdv.uni-lj.si/pajek/ (data zvernennya: ата звернення: 02.09.2020).
12. Biyachuyev, T.A. (2016), “Bezopasnost' korporativnykh setey” [Security of corporate networks] : ucheb. posobiye / T.A. Biyachuyev; pod red. Osovetskogo L.G. – SPb.: SPbGU ITMO, 161 p.
13. Bregg, R., Rods-Ousli, M., Strassberg, K. (2006) “Bezopasnost' setey. Polnoye rukovodstvo” [Network Security. Complete Guide] / R. Bregg, M. Rods-Ousli, K. Strassberg; – M : Ekom, 912 p.
14. Zavdada A.A. “Analiz suchasnykh system vyyavlennya atak i zapobihannya vtorhnennyam” [Analysis of of modern detection of attacks and prevention of invasions of systems] / A.A. Zavada, O.V. Samchyshyn, V.V. Okhrimchuk // Zbirnyk naukovykh prats′ ZHVI NAU «Informatsiyni systemy″12», 2012. – Vypusk 6, pp. 97 – 106.
15. Zahal′ni rekomendatsiyi shchodo pidvyshchennya rivnya zakhyshchenosti informatsiynykh resursiv pry viddaleniy roboti spivrobitnykiv ustanovy [General recommendations for improving the level of security of information resources in the remote work of employees of the institution] URL:
http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article;jsessionid=322B14F318F82FDEB1180D17FE0BFF97.app1?showHidden=1&art_id=320060&cat_id=317163 (date of application: 02.09.2020).
16. Kolotov, A. Network monitoring with tcpdump. URL: http://www.linuxshare.ru/docs/net/tcpdump.html (date of application: 02.09.2020).
17. Lukats'kiy, A.V. (2006), “Predotvrashcheniye setevykh atak: tekhnologii i resheniya” [Prevention of network attacks: technologies and solutions] / A.V. Lukatskiy. – SPb. : Ekspres Elektronika, p. 268.
18. Stollings, V. (2002), “Osnovy zashchity setey. Prilozheniya i standarty” [Fundamentals of Network Security. Applications and standards] / V. Stollings. – M.: Izdatel'skiy dom "Vil'yams", p.432.
19. Tropina M. Doslidzhennya sotsial′nykh merezh yak novoho fenomenu suchasnoho svitu [Research of social networks as a new phenomenon of the modern world] / M. Tropina // Naukovi zapysky Maloyi akademiyi nauk Ukrayiny. Seriya «Pedahohichni nauky» : [zb. nauk. prats′ ; redkol. : S.O. Dovhyy (holova), O.YE. Stryzhak, O.V. Lisovyy, I.M. Savchenko ta in.]. – Kyiv: Natsional′nyy tsentr «Mala akademiya nauk Ukrayiny», 2019. — Vyp. 16. – Pp. 57-63 (p. 76)

D.Sc. Lienkov S.V., Ph.D. Dzhulij V.M., D.Sc. Sieliykov O.V.,
Ph.D. Orlenko V.S., Atamaniuk A.V.

SECURITY MODEL DISSEMINATION OF FORBIDDEN INFORMATION IN INFORMATION AND TELECOMMUNICATION NETWORKS

The article proposes an approach to defining a security model for the dissemination of prohibited information in information and telecommunication networks.

The most effective prediction of the spread of the prohibited information threat is carried out by modeling this process. Information and telecommunication networks are large-scale networks with an ever-

growing number of subscribers. With the rapid growth in the number of ITKS users, there are problems of information security and information protection in them.

The analysis of information security problems proved that apart from the problems associated with the use of the global Internet as a distributed information and telecommunication system, it is well known and can be solved, there is a poorly studied problem of prohibited content.

Creation of models and algorithms for the spread of the threat of prohibited information is one of the key approaches to solving this problem. The analysis of publications on this topic shows that existing solutions are ineffective. Usually, when modeling the propagation of a threat of prohibited information, the ITKS topology (the network model is a fully connected graph) is not taken into account. When modeling the threat of the spread of prohibited information, it is important to have a topology that reflects the structure of connections in a real network, as well as to use an adequate model of information interaction between nodes. Another important problem is the large-scale ITCS, which makes it difficult to obtain data from the simulation model in a reasonable time. The solution to this problem is to create an analytical model of the threat of the spread of prohibited information in the ITCS.

An algorithm has been developed for the implementation of TSPI (threat of the spread of prohibited information) in the ITKS, based on the nature of the processes occurring in real conditions.

The simulation model of TSPI in ITKS has been proposed, which takes into account the topological characteristics of the network, as well as the features of information interaction of subscribers as man-machine systems. With its help, experiments have been carried out, the results of which have shown the dependence of the implementation of the RFID on the topological vulnerability of the network.

An analytical model of the TSPI has been developed, taking into account the topological vulnerability of the network. The relevance of the results of the analytical solution was confirmed by a series of experiments on the topology of a real network using simulation modeling. In this case, the error for the protection process was no more than 10%, for the attack process - no more than 15%.

Keywords: information security, analytical model, simulation model, threat propagation, information interaction, network model.