Система підтримки прийняття рішень для виявлення ознак загроз інформаційній безпеці держави у соціальних інтернет-сервісах та оцінювання їх рівня

Молодецька-Гринчук К.В.
кандидат технічних наук доцент,
доцент кафедри комп'ютерних технологій і моделювання систем,
Житомирський національний агроекологічний університет

На сучасному етапі розвитку інформаційного суспільства соціальні інтернет-сервіси (СІС) використовуються як ефективний інструмент комунікації учасників віртуальних спільнот, яких називають акторами [1, 2]. Завдяки наявності інструментарію для залучення широкої аудиторії до обговорення актуальних проблем різних галузей, об'єднання у групи за інтересами, координації громадянського суспільства для впливу на суспільне і політичне життя тощо СІС перетворилися на невід'ємну частину національного інформаційного простору держави. Одночасно СІС представляють собою джерело загроз інформаційній безпеці держави (ІБД) внаслідок поширення недостовірного або викривленого контенту в поєднанні з технологіями інформаційно-психологічного впливу на суспільну та масову свідомість [2]. У результаті проведених досліджень встановлено, що існуючі засоби і підсистеми ІБД у СІС не відповідають рівню сучасних загроз, тому розроблення дієвого наукового інструментарію для автоматизації процесів виявлення і протидії загрозам у СІС є актуальним теоретико-прикладним завданням.

Із праць [1, 3] відомо, що в основу системи забезпечення інформаційної безпеки (СЗІБ) покладено комплекс засобів забезпечення інформаційної безпеки, які застосовують адміністративно-правові, інформаційно-аналітичні, організаційно-управлінські та інші дії для сталого розвитку інформаційного середовища держави. При цьому СЗІБ є компонентом системи забезпечення національної безпеки і може складатися з підсистем для розв'язку окремих завдань. Встановлено, що одна з ключових ролей у забезпеченні ІБД відводиться Міністерству інформаційної політики України (МІПУ) [1]. Для реалізації визначених у Доктрині інформаційної безпеки України механізмів протидії сучасним загрозам і автоматизації процедур їх раннього виявлення та оцінювання необхідно розробити відомчі підсистеми інформаційної безпеки [3]. Тому для забезпечення заданого стану ІБД у СІС необхідно розробити систему підтримки прийняття рішень (СППР) як компоненту відомчої підсистеми забезпечення ІБД на основі запропонованих на попередніх етапах досліджень методів виявлення, оцінювання і протидії загрозам. Така СППР дозволить підвищити загальну ефективність СЗІБ держави у СІС, що додатково актуалізує обраний напрямок наукових досліджень.

Метою даної роботи є створення адекватної моделі СППР для виявлення ознак загроз ІБД у СІС і оцінювання їх рівня, що забезпечить автоматизацію процедур раннього виявлення, оцінювання та підвищить ефективність протидії загрозам. Для побудови СППР для виявлення ознак загроз інформаційній безпеці держави у СІС та оцінювання їх рівня на основі досліджень [3-5] запропоновано наступний алгоритм функціонування.

Етап І. Моніторинг текстового контенту СІС. На початковому етапі проводиться моніторинг інформаційного середовища СІС для виявлення контенту на задану тематику, який складається з таких кроків.

Крок 1.1. Визначення множини загроз інформаційній безпеці держави у СІС. Експерт з інформаційної безпеки на основі аналізу значущої і критичної тематики контенту у суспільстві визначає множину актуальних загроз у СІС.

Крок 1.2. Пошук текстового контенту СІС. Для пошуку у СІС текстового контенту, що ставить загрозу ІБД. Індексація текстового контенту СІС виконується з використанням методів інформаційного пошуку з урахуванням змісту контенту. Це дозволить знайти релевантний семантичному ядру текстовий контент і дані акторів, які його поширили.

Етап ІІ. Розрахунок частинних ознак загроз у відібраному текстовому контенті СІС. Відібраний на попередньому кроці текстовий контент і дані акторів досліджуються на ознаки застосування для проведення інформаційних операцій у СІС. З цією метою проводиться аналіз присутності організаційних, змістовних, маніпулятивних ознак у контенті та оцінюється профіль інформаційної безпеки акторів.

Крок 2.1. Виявлення організаційних ознак проведення інформаційних операцій. Встановлено, що проявом організаційних ознак інформаційних операцій у СІС є застосування спеціалізованого програмного забезпечення для поширення заданого контенту і використання соціальних ботів [3].

Крок 2.2. Встановлення змістовних ознак загроз. Проводиться аналіз відібраного текстового контенту з використанням семантичного аналізу на базі онтологій [3]. Для цього створюються онтологія з описом досліджуваної предметної області та семантичний опис відібраного текстового контенту. Детектування змістовних ознак загроз виконується з використанням сигнатурного методу і методу виявлення аномалій. У випадках високої релевантності текстового контенту семантичному ядру і відсутності у ньому виявлених змістовних ознак загроз він підлягає додатковому аналізу експертом з інформаційної безпеки для виявлення небезпечних семантичних конструкцій.

Крок 2.3. Виявлення маніпулятивних ознак загроз виконується відповідно до методики оцінювання маніпуляцій суспільною думкою у СІС [3]. Для текстового контенту встановлюються показники: сумнівності викладених фактів; емоційного забарвлення; тональності; сенсаційності; прихованої теми. На основі розрахованих показників визначається величина інформаційної ентропії маніпуляції суспільною думкою, який характеризує рівень невизначеності відносно застосування технологій прихованого впливу.

Крок 2.4. Оцінювання профілів інформаційної безпеки акторів СІС. На даному кроці проводиться дослідження профілів акторів [3]. Його суть зводиться до аналізу таких характеристик: атрибути профіля актора; показники активності публікації контенту; ознаки, властиві контенту профіля актора; аналіз зв'язків актора у СІС. Обчислені показники використовуються для подальшого визначення його конкретного класу загрози у результаті класифікації.

Крок 2.5. Розрахунок інтегральної оцінки ознак загроз інформаційній безпеці держави у СІС. Крок зводиться до багатокритерійної задачі оцінювання ознак загроз із різними ваговими коефіцієнтами. Виконується згортка виявлених на кроках 2.1−2.4 ознак загроз по нелінійній схемі компромісів професора А. М. Вороніна. Якісна оцінка рівня загрози визначається у результаті нормування скалярної згортки до мінімуму з подальшим переходом до якісної шкали оцінки [4].

Етап ІІІ. Протидія загрозам інформаційної безпеки держави у СІС. Залежно від отриманого на попередньому етапі значення інтегральної оцінки ознак загроз приймається відповідне рішення щодо протидії. Прийняття рішень виконується на основі моделі, розробленої у публікації [3]. У випадку виявлення загрози ІБД рівня «нижче середнього» виконується моніторинг загрози у інформаційному середовищі СІС відповідно до першого етапу алгоритму функціонування СППР. Якщо виявлено загрозу рівня «вища середнього» окрім моніторингу проводиться прогнозування поширення текстового контенту й запитів на нього. Для загроз рівня «існує» окрім моніторингу додатково реалізують синергетичне управління взаємодією акторів у СІС на основі розробленої концепції [5] для штучно-керованого переходу віртуальної спільноти до бажаного стану ІБД. На заключному кроці виконується вироблення практичних рекомендацій з протидії загрозам ІБД у СІС. Залучення окремих виконавчих державних органів проводиться залежно від сфери суспільної діяльності, на яку націлена виявлена загроза [3]. Рекомендації з протидії загрозам ІБД у СІС сформульовані на основі Доктрини інформаційної безпеки України і проведеного аналізу впливу загроз на сфери суспільної діяльності [3].

Вперше запропоновано модель СППР для виявлення ознак загроз ІБД у СІС та оцінювання їх рівня, яка є компонентом системи забезпечення ІБД і забезпечує автоматизацію процедур раннього виявлення та оцінювання загроз. Структурно СППР складається з таких модулів: моніторингу інформаційного середовища СІС; оцінювання частинних ознак загроз ІБД у СІС; прогнозування поширення акторами контенту і запитів на нього; інтегрального оцінювання ознак загроз; протидії загрозам у СІС. Перевагами розробленої моделі СППР є: врахування частинних ознак загроз ІБД у СІС для детектування різних варіантів прояву інформаційних операцій; визначення рівня загрози на основі

інтегрального показника за нелінійною схемою компромісів, що забезпечує досягнення компромісу між частинними критеріями та оптимальність рішення за Парето; прогнозування динаміки поширення контенту й запитів на нього за даними контент-аналізу повідомлень у СІС на основі метрики самоподібності для завчасного корегування вироблених управляючих дій СППР; застосування синергетичного управління взаємодією акторів СІС, що забезпечує запуск у віртуальних спільнотах процесів керованої самоорганізації акторів для переходу системи до заданого стійкого стану інформаційної безпеки держави. Таким чином досягається ефективність, оперативність і швидкодія функціонування системи забезпечення інформаційної безпеки держави у СІС, що є сьогодні вкрай актуальним завданням для України.

Література:

1. Грищук Р. В. Основи кібернетичної безпеки : монографія / Р. В. Грищук, Ю. Г. Даник; за заг. ред. проф. Ю. Г. Даника. – Житомир : ЖНАЕУ, 2016. – 636 с.

2. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції: навч. посіб. / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. – К. : КНТ, 2006. – 280 с.

3. Молодецька-Гринчук К. В. Модель системи підтримки прийняття рішень для виявлення ознак загроз інформаційній безпеці держави у соціальних інтернет-сервісах та оцінювання їх рівня / К. В. Молодецька-Гринчук // Безпека інформації. – 2017. – Т. 23, №2. – С. 136–144.

4. Молодецька-Гринчук К. В. Метод оцінювання ознак загроз інформаційній безпеці держави у соціальних інтернет-сервісах / К. В. Молодецька-Гринчук // Автоматизація технологічних і бізнес-процесів. – 2017. – Vol. 9, Iss. 2/2017. – С. 36–42.

5. Hryshchuk R. Synergetic control of social networking services actors' interactions / R. Hryshchuk, K. Molodetska // Recent Advances in Systems, Control and Information Technology. – Vol. 543. – Springer International Publishing, 2017. – PP. 34 –42.