2. Ріппа П.С. Забезпечення авторських прав у мережі Інтернет [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua
3. Вирок Перемишлянського районного суду Львівської області від 20.01.2017 року по справі № 449/613/15-к. [Електронний ресурс]. – Режим доступу: http://reyestr.court.gov.ua

Методика протидії інформаційним загрозам у кібернетичному просторі

Лагодний О.В.
ад'юнктнауково-організаційного відділення.
Житомирський військовий інститут імені С. П. Корольова
Грищук Р.В.
доктор технічних наук, с.н.с.,начальник
науково-дослідного відділу інформаційної
та кібернетичної безпеки наукового центру.
Житомирський військовий інститут імені С. П. Корольова

Нині стало очевидним істотне зростання ролі негативного інформаційного впливу (ІВ) у ході досягнення економічних, політичних, військових цілей державами-агресорами [1, с. 15]. Водночас, активний розвиток інформаційних технологій привів до якісного розуміння ролі і місця ІВ в системі забезпечення інформаційної та кібернетичної безпеки держави.

Агресія Російської Федерації [2, с. 2], інші докорінні зміни у зовнішньому та внутрішньому безпековому середовищі створюють передумови для подальшої інтенсифікації такого негативного явища, як кіберзлочинність. Тому протидія їй, у тому числі й у вигляді протидії інформаційним загрозам (ІЗ) у кіберпросторі (КП), є актуальним науковим та прикладним завданням.

Згідно зі Стратегією забезпечення кібербезпеки України на Національну поліцію України як суб'єкт забезпечення кіберпезпеки покладаються такі основні функції: забезпечення захисту прав і свобод людини та громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; запобігання, виявлення, припинення та розкриття кіберзлочинів; підвищення поінформованості громадян про безпеку в кіберпросторі [2, с. 4]. Саме забезпечення захисту прав і свобод людини та громадянина не може бути реалізованим без дієвих методик протидії ІЗ в КП [3, с. 3], [4, с. 114]. Розроблення таких методик потребує наявності точних даних про: рівень небезпеки ІЗ і пріоритетність у порядку нейтралізації; тенденцію і динаміку розвитку; критичні точки (точки біфуркації) та інтервали зміни динаміки розвитку тощо. Це дозволяє раціоналізувати розподіл сил і засобів протидії по цілях і за часом, а також підвищити адекватність планованих заходів, що реалізовуються, щодо нейтралізації виявлених ІЗ і недопущення їх переростання в інші більш небезпечні форми.

У зв'язку з цим актуальним є завдання з розроблення ефективних методик протидії ІЗ в КП спеціальними підрозділами кібербезпеки та кіберзахисту, у тому числі й підрозділами Національної поліції України. Варіант такої методики подано нижче.

Етап 1. Виявлення ознак ІВ в КП.

На цьому етапі проводиться виявлення перспективних джерел ІВ, формуються теми, за якими проводиться моніторинг джерел ІВ, та база статистичних даних за кожним напрямком. За результатами виконання даного етапу визначаються найбільш небезпечні джерела ІВ, напрямки за темами ІВ, створюється класифікатор за ознаками ІВ.

Етап 2. Оцінювання рівня ІЗ в КП.

На даному етапі здійснюється оцінювання кількісно-якісних показників ІВ за визначеними критеріями [5, с. 32].

Етап 3. Прогнозування розвитку ІЗ в КП.

На останньому етапі за допомогою використання бази статистичних даних, кількісно-якісних показників та даних статистичного аналізу [6, с. 312] проводиться прогнозування подальшого розвитку ІЗ в КП. У результаті прогнозування одержуються дані щодо можливих напрямків реалізації ІЗ в КП. Такий підхід дозволяє раціонально розподілити сили та засоби для протидії ІЗ.

Отже, використання інформаційних систем та технологій у боротьбі з кіберзлочинністю, розробка методик та автоматизація процесів виявлення, оцінювання і прогнозування ІЗ в КП можуть бути підґрунтям для створення інтегрованої системи оцінювання інформаційних загроз та оперативного реагування на них.

Література:

1. Світова гібридна війна: український фронт : монографія / за заг. ред. В. П. Горбуліна. – К. : НІСД, 2017. – 496 с.
2. Про Стратегію кібербезпеки України: Указ Президента України від 15 березня 2016 року № 96/2016.
3. Про Доктрину інформаційної безпеки України: Указ Президента України від 25 лютого 2017 року № 47/2017.
4. 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.
5. Левченко О. В. Методика оцінювання кількісних показників негативного інформаційного впливу / О. В. Левченко, О. М. Косогов, А. О. Сірик. // Сучасні інформаційні технології у сфері безпеки та оборони. – 2017. – №1(28). – С. 31–35.
6. Вентцель Е. С. Теория вероятностей / Е. С. Вентцель. – М. : Наука, 1969. – 576 с.

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.