ПОДХОД К ОЦЕНКЕ ПРИЗНАКОВ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА В СОЦИАЛЬНЫХ ИНТЕРНЕТ-СЕРВИСАХ

Молодецкая-Гринчук К. В.
Кафедра компьютерных технологий и моделирования систем, Житомирский национальный агроэкологический университет
Житомир, Украина
E-mail: kmolodetska@gmail.com

Сегодня социальные интернет-сервисы превратились в популярный инструмент коммуникации участников виртуальных сообществ – акторов. В случае распространения в социальных интернет-сервисах недостоверного контента они превращаются в источник угроз информационной безопасности. Отсутствие действенных подходов к оценке таких угроз создает условия для проведения информационных операций в интересах отдельных субъектов. Предложен подход к оценке признаков угроз информационной безопасности на основе скалярной свертки по нелинейной схеме компромиссов. Преимуществом такого подхода является компромисс между частными признаками угроз и оптимальность полученного решения по Парето. Эффективность подхода экспериментально подтверждена на примере реальной информационной акции в социальных интернет-сервисах.

Введение

Сегодня социальные интернет-сервисы (СИС) используются участниками виртуальных сообществ – акторами, для образования информационных связей с другими акторами, оперативного распространения собственного контента, самоорганизации с целью влияния на общественные и политические процессы в государстве [1, 2]. Однако, практический опыт использования СИС как средства массовой коммуникации показал, что они превратились в действенный инструмент проведения информационных операций и реализации угроз информационной безопасности личности, общества, государства [2].

В предыдущих исследованиях [2] установлено, что целью таких угроз может быть влияние на свободу выбора акторов СИС, распространение призывов к сепаратизму, свержению конституционного строя и тому подобное. Опыт гибридной войны против Украины продемонстрировал появление качественно новых и действенных технологий информационного воздействия на акторов СИС. Это привело к возникновению противоречия между уровнем новейших информационных технологий воздействия на акторов СИС и научным базисом оценки уровня угроз информационной безопасности государства. Поэтому возникает потребность в разработке действенных методов оценки уровня таких угроз для организации эффективного противодействия, которые будут положены в основу функционирования системы обеспечения информационной безопасности государства в СИС.

I. Признаки угроз информационной безопасности в СИС

Систематизация исследований [3-6], посвященных автоматизации процедур раннего выявления угроз информационной безопасности государства в СИС показала, что их признаками являются:

1. Организационные, указывающие на целевое использование информационных ресурсов и специального программного обеспечения в СИС для достижения поставленной цели;
2. Содержательные – наличие в контенте СИС деструктивного информационного посыла, который применяется для влияния на акторов виртуальных сообществ;
3. Манипулятивные, сводящиеся к применению технологий скрытого управления акторами СИС для проявления в них желаемых психических состояний, реакции на распространяемый контент, влияния на свободу выбора и т. п.;
4. Оценка профиля информационной безопасности актора, представляющая набор агрегированных характеристик профиля актора в СИС для определения уровня его угрозы как возможного участника информационных акций.

II. Оценка признаков угроз информационной безопасности в СИС

Предложенный подход к оценке признаков угроз информационной безопасности государства в СИС основывается на нелинейной схеме компромиссов [7] и сводится к следующему.

Этап 1. Расчет показателя I_1 на основе технологии обнаружения организационных признаков информационных акций в СИС. Технология [3] сводится к поиску дубликатов публикаций и комментариев в СИС, расчета показателя читабельности текстового контента и ведения диалога с акторами, которые являются авторами такого контента. Вывод о целенаправленной информационной акции формируется на основе обоб-

щенного показателя

$$I_1 = I_1^n \to B, B = \{0;1\}, n = 1. \quad (1)$$

Этап 2. Определение показателя I_2 наличия деструктивного информационного влияния в контенте СИС. Выявление таких скрытых информационных влияний основывается на методе, предложенном в публикации [4] и заключается в интеллектуальном поиске текстового контента СИС в соответствии с заданным семантическим ядром по критерию актуальности, критичности и уровню обсуждения в обществе. Отобранный контент подлежит семантическому анализу на основе онтологий с использованием сигнатурного метода и метода выявления аномалий. В результате формируется показатель

$$I_2 = I_2^n \to B, B = \{0;1\}, n = 1. \quad (2)$$

Этап 3. Оценка проявления I_3 признаков манипуляций общественным мнением в СИС. Расчет показателя производится в соответствии с разработанной методикой выявления манипуляций общественным мнением [5]. Обобщение частных признаков манипуляций выполнено на основе оценки информационной энтропии H_n контента СИС, то есть установления уровня неопределенности относительно использования технологий скрытого воздействия на акторов

$$I_3 = 1 - H_n, H_n \in [0;1]. \quad (3)$$

Этап 4. Оценка I_4 профиля информационной безопасности актора. Расчет показателя реализован с использованием метода построения профилей информационной безопасности акторов [6]. Предложенный метод основан на технологиях интеллектуального анализа данных, в частности методах машинного обучения с учителем. Показатель I_4 принимает значения в диапазоне

$$I_4 \in [0;1]. \quad (4)$$

Этап 5. Определение весовых коэффициентов $[\alpha_j]$ признаков угроз информационной безопасности государства в СИС. Значения устанавливаются экспертами на основе их индивидуальных предпочтений и соответствуют оперативной ситуации в СИС [7]. Весовые коэффициенты угроз информационной безопасности $[\alpha_j]$ в СИС рассчитывают согласно выражению

$$\alpha_j = \frac{f_j}{\sum_{i=1}^{4} f_i}, j \in [1;4],$$

где f_j – оценка приоритетности признака угрозы, которую устанавливает эксперт.

Этап 6. Скалярная свертка признаков угроз по нелинейной схеме компромиссов. Многокритериальная задача оценки (1)–(4) сводится к модели векторной оптимизации с различными весовыми коэффициентами признаков угроз информационной безопасности государства в СИС [7]

$$I^* = \arg\min \sum_{j=1}^{4} \alpha_j (1 - I_j)^{-1}. \quad (5)$$

Признаки I_1 и I_2 принимают только предельные значения 0 или 1, что характеризует высокий уровень напряженности ситуации в СИС [7]. С целью исключения необходимости деления на ноль в выражении (5) для значений признаков равных 1 необходимо использовать величину 0,95.

Также проведено экспериментальное исследование предложенного подхода к оценке признаков угроз на примере реальной информационной акции в микроблоге Twitter. Полученные результаты совпадают с выводами международных организаций и доказывают его действенность и эффективность.

Выводы

Впервые предложен подход к оценке признаков угроз информационной безопасности государства в СИС, основанный на нелинейной схеме компромиссов, который отличается от известных подходов применением методов выявления признаков информационных акций в виртуальных сообществах. Разработанный подход положен в основу функционирования системы обеспечения информационной безопасности государства в СИС, что позволило автоматизировать процедуры раннего выявления угроз. Таким образом достигается оперативность и быстродействие системы обеспечения информационной безопасности государства в СИС.

III. Список литературы

1. Грищук, Р. В. Основи кібербезпеки / Р. В. Грищук, Ю. Г. Даник // – Ж.: ЖНАЕУ, 2016. – 688 с.
2. Молодецька, К. В. Соціальні інтернет-сервіси як суб'єкт інформаційної безпеки держави / К. В. Молодецька // Information technology and security. – 2016. – Vol. 4, Iss. 1. – С. 13–20.
3. Молодецька, К. В. Технологія виявлення організаційних ознак інформаційних операцій у соціальних інтернет-сервісах / К. В. Молодецька // Проблеми інформаційних технологій. – 2016. – № 20. – С. 84–93.
4. Молодецька-Гринчук, К. В. Виявлення інформаційних впливів у соціальних інтернет-сервісах на основі інтелектуального аналізу текстового контенту / К. В. Молодецька-Гринчук // Актуальні питання забезпечення кібербезпеки та захисту інформації. – 2017. – С. 121–122.
5. Молодецька-Гринчук, К. В. Методика виявлення маніпуляцій суспільною думкою у соціальних інтернет-сервісах / К. В. Молодецька-Гринчук // Інформаційна безпека. – 2016. – № 24. – С. 80–92.
6. Молодецька-Гринчук, К. В. Метод побудови профілів інформаційної безпеки акторів соціальних інтернет-сервісів / К. В. Молодецька-Гринчук // Інформаційна безпека. – 2017. – № 26. – С. 104–110.
7. Воронин, А. М. Многокритериальный синтез динамических систем / А. М. Воронин // Киев: Наукова думка, 1992. – 160 с.