VI. Методы моделирования и принятия решений при управлении безопасностью сложных систем

Кереселидзе Н.Г.

Модель информационной безопасности в случае двух источников дезинформации

Аннотация: Рассматривается вопрос моделирования информационной безопасности общества в условиях нескольких источников дезинформации. Один из которых функционирует непосредственно внутри общества, а другой воздействует на членов общества извне. Для описания распространения дезинформации в обществе и борьбы с ней выбрана математическая и компьютерная модель. Построенная Математическая Модель описывает функционирование динамической системы.

Ключевые слова: математическая и компьютерная модель, динамическая система, дезинформация, информационная безопасность, борьбы с дезинформациями

Введение

В демократических обществах, где курс развития страны, безопасности, внутренней, внешней политики и т.д. определяется участием электорального населения в выборах, крайне важно, чтобы электоральное население участвовало в выборах в среде, как можно с меньшим количеством дезинформации. Дезинформация может привести к тому, что избиратели будут принимать предвзятые решения, основанные на заблуждениях, которые будут вредны или катастрофичны для развития страны. Определенный момент времени число людей, воспринявших фейковую информацию и находящихся под ее влиянием, может быть разным. Стоит вопрос – какое число адептов ложной информации считать

критическим в развитии общества? Если учесть опыт многих демократических стран, установивших барьер прохождения в парламент для политических партии, то естественно считать, что в обществе 5% адептов ложной информации уже можно считать оранжевым уровнем информационной опасности. Так как эти адепты ложной информации в случае выборов, могут провести парламент своих представителей и тем самым, активно участвовать в политической жизни страны. Если же число адептов около сорока процентов, то их представители в парламенте могут создать правящую коалицию, и тем самым получаем красный уровень общественной опасности. Таким образом, целью борьбы с дезинформацией должно быть удержание количества адептов ложной информации ниже пяти процентов электората.

1. Постановка задачи

В обществе с численностью N человек в каждый момент времени $t \in [0,T]$ распространяют потоки информации три источника в отличии от работ [1], [2], где рассматриваются лишь два источника потока информаций. Источник О2, находясь непосредственно в обществе, распространяет ложную информацию объеме $y_5(t)$. Источник О3, находясь вне общества, распространяет ложную информацию объеме $y_6(t)$. Источник О1, находясь непосредственно в обществе, распространяет антиложную, правдивую информацию объеме $y_4(t)$, и тем самим старается помочь членам общества освободится от влияния ложной информации. Источник О1, введет борьбу с дезинформацией от источника О2 только информационными потоками, а с источником О3, помимо информационных потоков, теми средствами, которые физически препятствуют распространению информации от источника О3 в обществе. Например, аннулируя лицензию на вещание, запрет провайдерам сотрудничать с источником О3, создавая радиотелевизионные помехи, если источник О3 использует для распространения ложной информации радиотелевизионный каналы. Все три источника информационных потоков стараются привлечь каждого члена общества в свои сторонники. Таким образом, распространение дезинформации и борьба с ней разделяют

общество на группы. Например: риск группа RG – Y_1, с количеством членов $y_1(t)$, которые еще не определились за каким источником будут следовать; Первая группа адептов AG – Y_2, с количеством членов $y_2(t)$, которые стали адептами источника O2; Вторая группа адептов AG1 – Y_7, с количеством членов $y_7(t)$, которые стали адептами источника O3; Группа Иммунитета – $IG - Y_3$, с количеством членов $y_3(t)$, которые самого начала, либо позже отвергли ложную информацию от источников O2 и O3.

Структурно переход людей из одной группы в другую под воздействием ложной и антиложной информации можно изобразить следующим образом (рисунок 1).

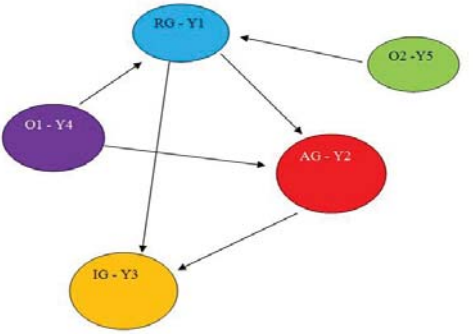

Рисунок 1 – Источники информации и группы с указанием переходов

Как видно из рисунка 1, источник O2 и O3 воздействует только на группу Риска, а источник O1, помимо группы Риска, воздействует также на группы Адептов – AG и AG1. Источник O1 действует с целью сокращения численности Адептов путем распространения антиложной информации. Однако создание и распространение одной единицы антиложной информации требует определенных финансовых и иных ресурсов. Вполне возможно, что при определенных ограниченных ресурсах источник O1 не сможет сократить численность группы Адептов. Поэтому возникает задача определения необходимого количества ресурса источник O1 для

сокращения численности Адептов и при этом эффективного использования этих ресурсов. Т.е. возникает задача оптимального управления борьбой с ложной информацией.

2. Решение задачи

Из группы Риска (Y_1) в результате воздействия ложной информации ($y_5(t)$) ее члены могут выйти из нее и перейти в группу Адепт (Y_2), под воздействием ложной информации ($y_6(t)$) ее члены могут выйти из Риска и перейти в группу Адептов AG1 (Y_7), а под воздействием антиложной информации ($y_4(t)$) в группу Иммунитет (Y_3). Межличностные отношения членов групп Риска и Адептов также влияют на переход из группы Риска в группу Адептов. А межличностные отношения членов групп Риска и Иммунитета влияют на переход из группы Риска в группу Иммунитет. Заметим, что численность членов группы Риска не увеличивается, функция не растет. Аналогично можно подойти и к другим группам. В результате получим динамическую систему борьбы с дезинформацией в обществе:

$$
\begin{cases}
\dfrac{dy_1(t)}{dt} = -\lambda(t)y_4(t)y_1(t) - \kappa(t)y_5(t)y_1(t) - \gamma_1(t)y_6(t)y_1(t) - \\
-\alpha_1(t)y_1(t)y_2(t) - \alpha_2(t)y_1(t)y_3(t) - \alpha_3(t)y_1(t)y_7(t), \\
\dfrac{dy_2(t)}{dt} = \alpha_1(t)y_1(t)y_2(t) + \kappa(t)y_5(t)y_1(t) - \\
-\lambda_1(t)y_4(t)y_2(t) - \gamma(t)y_2(t) - \beta_1(t)y_2(t)y_3(t), \\
\dfrac{dy_7(t)}{dt} = \alpha 1_1(t)y_1(t)y_7(t) + \kappa 1(t)y_6(t)y_1(t) - \\
-\lambda 1_1(t)y_4(t)y_7(t) - \gamma 1(t)y_7(t) - \\
-\beta 1_1(t)y_7(t)y_3(t), \\
\dfrac{dy_3(t)}{dt} = \gamma(t)y_2(t) + \alpha_2(t)y_1(t)y_3(t) + \beta_1(t)y_2(t)y_3(t) + \\
+\lambda_1(t)y_4(t)y_2(t) + \gamma 1(t)y_7(t) + \beta 1_1(t)y_7(t)y_3(t), \\
\dfrac{dy_4(t)}{dt} = \omega_1(t)y_2(t)y_7(t)\left(1 - y_4(t)/M_1\right), \\
\dfrac{dy_5(t)}{dt} = \omega_2(t)y_1(t)\left(1 - y_5(t)/M_2\right), \\
\dfrac{dy_6(t)}{dt} = u(t)\omega_3(t)y_1(t)\left(1 - y_6(t)/M_3\right).
\end{cases}
\qquad (1)
$$

где все коэффициенты системы (1), кроме $u(t)$, положительны и переменны. Параметры M_1, M_2, M_3 соответствуют уровням тех ИТ, с помощью которых соответствующим образом распределяются потоки информации по операторам. Параметр $u(t)$ определяет, насколько блокируется поток информации внешнего источника, используя метод помех, запретов и др. Его значение может быть и

отрицательным. Предположим, что в начальный момент времени известны численность всех групп и объемы потоков операторов, т.е.

$$\begin{cases} y_1(0) = y_{10}, \quad y_2(0) = y_{20}, & y_3(0) = y_{30}, \\ y_4(0) = y_{40} \quad y_5(0) = y_{50} \quad y_6(0) = y_{60}, \quad y_7(0) = y_{70}. \end{cases} \tag{2}$$

Таким образом, была построена математическая модель распространения дезинформации двумя источниками и борьбы с ней в виде задачи Коши (1), (2), где (2) – начальные условия для динамической системы (1).

Значения функции $y_2(t)$, $y_7(t)$ определяет, насколько дезинформация проникла в общество. Обычно пять процентов – это барьер в некоторых европейских странах, который политические деятели должны преодолеть на выборах, чтобы попасть в законодательный орган. Если выборы назначены на время T, то к этому времени число приверженцев источников О2 и О3 — $y_2(T)$ и $y_7(T)$, соответственно, должно быть меньше пяти процентов избирателей. Пусть число избирателей совпадает с численностью общества, тогда должно быть выполнено следующее:

$$y_2(T) + y_7(T) < N / 20. \tag{3}$$

Таким образом, возникает задача – динамическая система должна быть переведена из состояния (2) в состояние (3) так, чтобы общество, в основном свободное от дезинформации, сделало выбор. Для перевода системы из состояния (2) в (3) в рабочем состоянии предлагается рассматривать как управляющие параметры объем потока первого источника и $u(t)$ – создание помех для распространения ложной дезинформации О3 источником. Тем самым мы получаем задачу оптимального управления борьбой с дезинформацией:

$$J(\omega_1(t), M_1, u(t)) = \int_0^T (\phi(t) y_4(t) + \phi_1(t) u(t)) dt \to inf. \tag{4}$$

где $\phi(t)$ – цена распространения одной единицы антиложной информации в конкретный момент времени, а $\phi_1(t)$ – цена одной единицы помех для дезинформации О3 источника. Таким образом, задача оптимального управления борьбой с двумя источниками дезинформацией – (4), (1) – (3) имеет следующий смысл. Оператор 1 должен производить такой объем антиложной информации и создать такие помехи для источника О3, которые удовлетворят систему (1), граничным значениям (2), (3), и цена ее создания будет минимальной.

3. Выводы

Исследуя вопрос управляемости задачи (4), (1) – (3) с помощью компьютерного моделирования, используя пакет прикладных программ MatLab можно заключить. Для информационной безопасности общества недостаточно сократить число приверженцев дезинформации только в определенный момент времени, например, перед каким-либо голосованием. В некоторые моменты влияние дезинформации на общества может быть настолько сильным, что общество в целом может легитимировать революционные, досрочные парламентские, президентские выборы и т.д. Поэтому в задаче оптимального управления борьбой с дезинформацией, необходимо контролировать число приверженцев ложной информации на протяжении всего периода времени.

Литература:

1. *Кереселидзе Н.Г.* Об одном аспекте информационной безопасности в модели борьбы с дезинформацией / Проблемы управления безопасностью сложных систем: материалы XXXI Международной научной конференции (ПУБСС'2023, Москва). – М.: ИПУ РАН, 2023. – С. 174-179. – DOI: 10.25728/iccss.2023.94.99.022.

2. *Kereselidze N.* Mathematical and Computer Modeling of a Dynamic System for Effectively Combating Disinformation // WSEAS Transactions on Systems. – 2024. – Vol. 23. – P. 66-72. – DOI: 10.37394/23202.2024.23.7.