УДК 004.056

А.В. Дудатьев

КОМПЛЕКСНЫЙ МЕТОД ПРОТИВОДЕЙСТВИЯ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИМ ОПЕРАЦИЯМ

Введение

Современные социотехнические системы являются одновременно объектами и субъектами в информационном пространстве для проведения специальных информационных операций (СИО) в форме информационно-психологических операций (ИПО) и информационно-кибернетических операций (ИКО), которые в свою очередь выступают механизмами ведения информационной войны. Главная цель информационной войны — перепрограммирование сознания человека, и как результат, изменение состояния его сознания, отношения к социуму, окружающей среде, выполняемой работе и т.д. Иными словами, основная цель ИПО — создание «нужного» специально «подготовленного» человека или группы людей как элемента социальной части социотехнической системы (СТС) путем ее информационного инфицирования. Специалисты сравнивают эффективность проведения ИПО с оружием массового уничтожения. Поэтому для эффективной жизнедеятельности СТС, выполнения системой своих задач необходима организация комплексной информационной защиты социальной части СТС, суть которой — защита собственных информационных ресурсов от несанкционированного доступа и защите от деструктивного информационного влияния. Эффективное управление комплексной информационной безопасностью позволит реализовать необходимую самоорганизацию системы, что является актуальной задачей.

Анализ механизмов реализации и распространения ИПО

Информационное воздействие на социальную часть СТС может быть реализовано с помощью многих механизмов, подробно изложенных в [1]. Основная проблема, которая решается с использованием того или иного механизма проведения ИПО — так называемое «ненасильственное перепрограммирование» сознания социальной части СТС. Эта проблема в принципе была решена Р. Докинзом [2], который впервые ввел понятие культурного гена социума — мема. Мем определяется как минимальное количество информации в сознании человека, предназначенное для его культурной эволюции. С точки зрения информационной безопасности, мем может использоваться как раз для решения задачи «перепрограммирования сознания» человека или, другими словами, мемом можно назвать специально созданное информационное сообщение, распространяемое в информационном пространстве и предназначенное для формирования необходимой модели поведения и принятия соответствующих решений социальной части СТС. Мем может быть представлен в виде текстовой информации, специального движения, звукового сигнала, сочетания цветов одежды, определенных движений и т.д.

 ISSN 0572-2691

Существует недостаточно развитая теория качественного и количественного оценивания и понимания процесса подготовки, распространения и воздействия, специально созданного мема на объект воздействия. Например, различные источники массовой информации, которые можно рассматривать как источники информационного воздействия, распространяющие информацию на одну и ту же тему, но по-разному ее представляющие, могут влиять на состояние социума СТС.

В работе [3] анализируется процесс прохождения информации через так называемые три слоя распространения информации: новостные статьи (первичная или исходная информация), освещение этих статей в различных социальных медиа и комментарии по представленной информации. Очевидно, что под новостными статьями подразумевается специально подготовленная информация. Проходя через эти три слоя, первичная информация может быть изменена в силу различных причин, в том числе специально искажена. Иными словами, первоначальные акценты, сформулированные в виде специальных мемов и содержащиеся в первичных новостных сообщениях, могут быть смещены и, наоборот, созданы новые акценты, сформулированные в виде других мемов.

Существует так называемое рефлексивное управление, которое осуществляется навязыванием ложной мотивации. С точки зрения ведения информационной войны, весьма интересен важный аспект рефлексивного управления. Так, С. Леоненко утверждает, что во многих случаях решения принимаются машинами, т.е. технической частью СТС, которые не способны, как человек, реагировать на состояние и изменение окружающей среды, в том числе информационной, технологической, производственной, экологической и т.п. [4]. В этом случае происходит воздействие на технические средства сбора, обработки, передачи и отображения информации в целях навязывания оппонентам своих взглядов, т.е. фактически речь идет о влиянии программно-технической составляющей на человека и, как следствие, на процесс подготовки и принятия решения. Однако известны случаи, когда воздействие на техническую составляющую СТС возможно только при наличии специально подготовленного или заинтересованного человека. Характерным примером может быть использование вирусов группы StuxNet для противодействия иранской ядерной программе [5].

В работе [6] автор предлагает методологию комплексной защиты человека и социальных групп от негативного информационно-психологического влияния, суть которой заключается в адаптации субъектов воздействия в организованной социальной среде. Однако представленные исследования базируются на результатах состояния человека, т.е. фактически на последствиях проведенных ИПО, без учета непосредственной причины изменений социальной части СТС — специально подготовленной информации или мема, т.е. без учета этапов жизнедеятельности мема: этапа его проектирования, распространения и его сопровождения теми или иными средствами распространения информации, например в виде различных комментариев.

Исходя из представленной объективной картины реализации различных сценариев ведения информационной войны, одной из технологий которой является ИПО и ИКО, необходимо построить универсальный и комбинированный метод противодействия СИО, учитывающий все этапы специально подготовленной информации для проведения СИО.

Цель данного исследования — разработка комплексного метода противодействия специальным информационным операциям, учитывающего все этапы жизнедеятельности специально подготовленной информации — мема.

Задачами исследования являются:

— разработка метода защиты от ИПО на этапе ее подготовки или на этапе проектирования деструктивного мема;

— разработка метода защиты после проведения ИПО или этапе распространения и сопровождения деструктивного мема.

Модели реализации противодействия информационно-психологическим операциям

Существует множество причин, из-за которых могут возникнуть информационные войны. Основные из них:

— использование различных критериальных моделей для оценок процессов, событий, реально происходящих в различных сферах жизнедеятельности человека и т.д.;

— борьба за различные ресурсы, в том числе энергетические, научно-технические, социальные;

— геополитические интересы.

Поскольку потенциальный объект защиты находится в конкурентной информационной среде, можно допустить, что против него уже планируются или проектируются новые ИПО, проводятся различные ИПО в реальном времени и реализуется сопровождение или соответствующее комментирование специально подготовленной информации в виде мемов.

Анализ документа под названием «Протоколы собраний сионских мудрецов» раскрывает главный практический аспект информационной войны: контроль над системой управления [7]. Для современных социотехнических систем этот аспект многоуровневый и многоаспектный. Применение различных компонентов гибридной войны — экономическое противостояние, так называемые временные ограничения на торговлю и т.п.; контроль над системой голосования (всеобщее голосование). Например, управление комплексной информационной безопасностью на уровне «предприятие–регион–государство»; перепрограммирование населения или социальной части (сотрудника или группы сотрудников того или иного предприятия) СТС, применение различных средств массовой информации, рекламы, социальных сетей и т.д., терроризм как средство запугивания или выведения той же системы управления из состояния равновесия.

В [8] автор приводит три составные части информационной войны: стратегический политический анализ, информационное воздействие, информационное противодействие или защита. Однако более адекватную картину проведения информационной войны дополнит такой этап, как необходимое сопровождение или комментирование представленной информации — мема — с учетом различных источников информационного воздействия, возможностей доступа к ним, специфики аудитории, на которую данный мем спроектирован и т.п. Кроме того, введение данного этапа позволит выполнить рекомендации международного стандарта ISO/IEC 27001:2013, который был разработан с целью установить требования для создания, внедрения, поддержания функционирования и непрерывного улучшения системы менеджмента информационной безопасности.

Исходя из этого, предложены следующие составные части информационной войны.

1. Анализ информационного пространства. Эта часть предполагает сбор, обработку и обмен информацией о потенциальных противниках и союзниках для дальнейших активных действий. На этом этапе со стороны противника предполагается проектирование новых информационных воздействий — мемов, в целях их дальнейшего распространения.

2. Информационное воздействие. Данный этап предполагает распространение и внедрение подготовленной специальной информации в информационное поле противника, а также пресечение попыток противника получить нужную ему информацию.

3. Сопровождение или комментирование информационного сообщения — мема. Данный этап предполагает учет специфики источников распространения информационного сообщения — мема, специфику социальной части СТС, на которую данная информация распространяется. Другими словами, на этом этапе практически реализуется первенство и обеспечивается эффективность трактовки распространяемой информации.

4. Информационное противодействие или защита. Этап предполагает блокирование и компенсацию деструктивного информационного воздействия, которое распространяет и внедряет потенциальный конкурент или противник.

Данные этапы практически представляют последовательность определенных специальных информационных операций технологического процесса ведения информационной войны или конкурентной борьбы и соответствующей комплексной защиты, которая может проводиться на различных уровнях управления комплексной информационной безопасностью. Схема, представляющая процесс реализации комплексной защиты от проведения ИПО, показана на рис. 1.

Рис. 1

На основе предложенных этапов проведения информационной войны предлагается построение нового комплексного метода, связанного непосредственно с построением комплексной защиты на всех этапах проведения ИПО.

Предлагаемый метод предполагает построение комплексной защиты в два этапа.

1. Реализация комплексной защиты от реализации ИПО с применением упреждающего мема. Для реализации эффективного противодействия необходимо знать те места (ресурсы), против которых могут быть реализованы эти ИПО. Для этого необходимо выполнить анализ объекта защиты, определить минимальные и максимальные риски потенциальных ИПО и, исходя из этого, сформировать так называемые упреждающие мемы. Поскольку мемы направлены против социальной части СТС, то и информационное упреждение должно быть для социума.

В общем виде математическую модель объекта, находящегося в условиях информационного влияния, можно охарактеризовать множеством параметров, например:

$$O = \{O_s, O_r, O_d, t\}, \tag{1}$$

где O_s — состояние системы (защищенный или незащищенный), O_r — ее ресурсы, O_d — скорость работы системы, t — реальное время. В общем случае для идентификации объекта защиты можно использовать и другие параметры, наиболее важные для конкретного объекта.

Субъект информационного взаимодействия может характеризоваться такими параметрами:

$$S = \{S_m, S_r, S_z, S_{\text{oper}}, t\}, \tag{2}$$

где S_m — цели субъекта, S_r — его ресурсы, S_z — средства, S_{oper} — возможные действия субъекта, t — реальное время.

Для обеспечения устойчивого функционирования объекта защиты или для обеспечения его эффективной защиты от проведения ИПО необходимо обеспечить упреждающее определение вероятных деструктивных операций со стороны потенциального противника. С учетом условий информационного взаимодействия противоборствующих сторон, этапов проведения информационной войны предлагается такая методика для определения возможностей проведения ИПО и минимизации рисков.

1. Анализируются структура, элементы, внутренние и внешние связи объекта защиты. Определяются наименее защищенные места объекта зашиты, а также множество возможных информационных операций, проводимых в системе «объект–субъект». Выполняется анализ рисков и рассчитывается ранг соответствующих информационных операций: D_S — со стороны субъекта информационного взаимодействия и D_O — множества возможных операций противодействия со стороны объекта информационного взаимодействия [9].

2. Анализ рангов вероятных ИПО позволит определить множество специальных информационных операций, проведение которых может привести к максимальным или недопустимым рискам. Это позволит получить множество специальных ИПО, проводимых субъектом информационного взаимодействия — S_{oper}, реализация которых приведет к недопустимым рискам, т.е.

$$S_{\text{oper}_i} = \max(R_i), \tag{3}$$

где R_i — риск от проведения i-й операции S_{oper}.

3. Анализ множества специальных ИПО, приводящих к максимальным значениям риска, позволят сгенерировать множество упреждающих мемов со стороны объекта информационного взаимодействия O_{oper}.

Обобщая приведенные операции информационного противодействия, следует отметить, что сгенерированные упреждающие мемы рассчитаны на минимизацию вероятного информационного воздействия со стороны вероятного противника на этапе проектирования мемов. Таким образом, упреждающие мемы или упреждающая защита должны опережать во времени реализацию вероятных ИПО со стороны потенциального противника.

2. Реализации комплексной защиты от реализации ИПО предполагает применение компенсирующего мема. Используя теорию меметики, будем считать изменения состояния информационной среды результатом наличия в нем нового мема или мема, на факт присутствия которого отсутствует адекватная реакция. Результатом обслуживания нового мема является его нейтрализация или формирование адекватной защиты, а факт отсутствия нейтрализации этого мема будем считать эффективно проведенной ИПО, способной вывести СТС из состояния равновесия.

Поскольку оценка текущего состояния уровня защищенности получена в виде вероятностных оценок, процесс минимизации последствий, проведенных ИПО, рационально представить в виде вероятностных соотношений [9, 10].

Пусть имеется k источников распространения деструктивного мема (источников влияния). При этом i-й источник направляет влияние на n_i объектов социальной части СТС. Пусть также вероятность подпадания под влияние i-го источника равна P_i. Учитывая это, количество M_{MD} объектов социальной части СТС, подпавших под влияние деструктивного мема, вычисляется по формуле

$$M_{MD} = \sum_{i=1}^{k} p_i n_i. \tag{4}$$

Пусть для нейтрализации результата влияния деструктивного мема используется m источников распространения компенсирующего мема, из которых j-й источник направляет влияние на n_i объектов социальной части СТС. Пусть вероятность нейтрализации j-м источником равна q_j. Тогда с учетом модели для оценки эффективности информационного воздействия, предложенной в [10], количество M_{KM} объектов социальной части СТС, возвратившихся в состояние до проведения ИПО, определяется по формуле

$$M_{KM} = \sum_{i=1}^{m} q_1 n_1 = q_1 v_i^j (Dm) = \sum_{i,j,m=1}^{s} q_i (Y_m(P_j) / \left| D_m \right| K_t, \tag{5}$$

где v_i^j показывает принадлежность источника влияния к i-му классу, который использует j-й механизм реализации информационных операций; $Y_m(P_j)$ — количество объектов m-го класса, которые изменили свое состояние под действием j-го механизма влияния; K_t — коэффициент, который учитывает частоту обращения к данному источнику влияния и меняется от 0 до 1; s — количество классов и механизмов влияния.

Компенсирующий мем позволит минимизировать последствия проведенной ИПО с учетом принадлежности источника воздействия к тому или иному классу, например телевидение, печатные СМИ, социальные сети, а также механизм реализации ИПО.

Международный стандарт ISO/IEC 27001:2013 указывает на то, что организация должна определить внешние и внутренние проблемы, значимые с точки зрения ее целей и влияющие на способность достигать ожидаемых результатов ее системы менеджмента информационной безопасности. Организация должна определить и выполнить процесс обработки рисков информационной безопасности с целью: выбрать соответствующие методы обработки рисков информационной безопасности с учетом результатов оценки рисков; определить любые средства управления, необходимые для реализации выбранных методов обработки рисков информационной безопасности. Данные рекомендации формализованы на первом этапе предлагаемого метода. Второй этап фактически реализует возможность синтеза системы управления комплексной безопасностью с учетом выполнения требований, изложенных в разд. 6 данного стандарта, и возможностью дополнения необходимых средств управления информационной безопасностью. В данном методе это сочетание упреждающих и компенсирующих мемов.

Структурная схема предложенного метода представлена на рис. 2, где P_i — вероятность проведения той или иной ИПО, R_{ng_i} — ранг *i*-й ИПО, R_i — риск от проведения *i*-й ИПО.

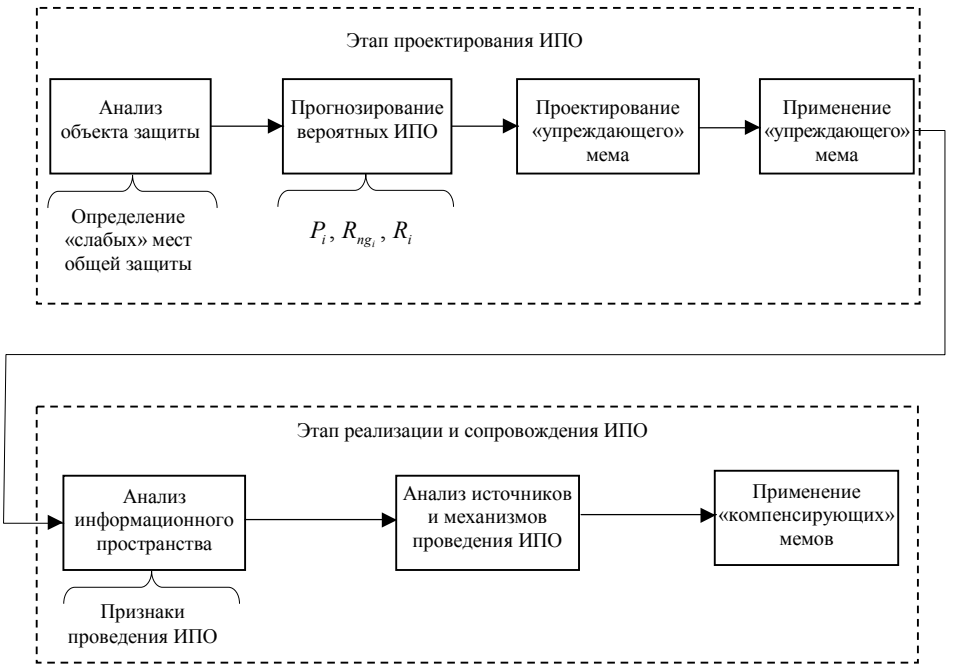

Рис. 2

Заключение

Для того чтобы победить организованного и квалифицированного противника в информационном противостоянии, а также эффективно противостоять организованным ИПО, необходимо учитывать все этапы жизнедеятельности специально созданной деструктивной информации. Разработанный метод должен быть интегрирован в системную организацию комплексного противодействия. Представленный метод, учитывающий технологические особенности реализации проведения ИПО, предлагается реализовать в структуре ситуационного центра для управления комплексной информационной безопасностью на уровне «предприятие–регион–государство». Предложенный метод позволяет эффективно решать задачи по управлению комплексной информационной безопасностью в соответствии с ISO/IEC 27001:2013, а также НДТЗІ 1.4-001-2000 (Приложение, п. 1) с учетом специфики этапов проектирования, реализации и сопровождения специального деструктивного мема.

А.В. Дудатьєв

КОМПЛЕКСНИЙ МЕТОД ПРОТИДІЇ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИМ ОПЕРАЦІЯМ

Технології інформаційної війни принципово змінюють підходи до вирішення задач оцінювання та забезпечення комплексної інформаційної безпеки. Актуальною проблемою є реалізація захисту соціуму від спеціальних інформаційно-психологічних операцій. Запропоновано комплексний метод

захисту від деструктивних інформаційних впливів, який враховує етапи проектування, розповсюдження і супроводу умовної одиниці інформаційно-психологічного впливу — мема.

A.V. Dudatyev

COMPLEX METHOD OF INFORMATIONAL-PSYCHOLOGICAL OPERATIONS COUNTERACTION

Informational war technologies fundamentally change approaches to problems solutions yielding complex information security evaluation and provision tasks. The implementation of the society protection from special informational-psychological operations is important problem. The complex method of the protection from destructive informational impacts, covering designing, spreading and supporting stages of informational-psychological impact unit — meme, is proposed.

1. *Остапенко Г.А.* Информационные операции и атаки в социотехнических системах. — М. : Горячая линия–Телеком, 2007. — 134 с.
2. *Докинз Р.* Эгоистичный ген. — М. : Мир, 1993. — 318 с.
3. *Chenhao Tan, Adrien Friggeri, Lada A. Adamic.* Lost in propagation? Unfolding news cycles from the source // Proceedings of the Tenth International AAAI Conference on Web and Social Media (ICWSM 2016). — 2016. — P. 378–387.
4. *Леоненко С.* Рефлексивное управление противником // Армейский сборник. — 1995. — № 8. — С. 27–32.
5. *Андрєєва О.М., Мусієнко К.* Кіберзброя та аналіз її деструктивної діяльності на прикладі впливу вірусу нового покоління StuxNet на іранську ядерну програму // Актуальні проблеми міжнародних відносин. — 2011. — Вип. 103(1). — С. 29–34. — htpp://nbuv.gov.ua/UJRN/apmv
6. *Шиян А.А.* Методологія комплексного захисту людини та соціальних груп від негативного інформаційно-психологічного впливу // Безпека інформації. — 2016. — № 1. — С. 94–98.
7. *Расторгуев С.П.* Философия информационной войны. — М. : Аутоплан, 2000. — 444 с.
8. *Панарин И.Н.* Первая мировая информационная война. Развал СССР. — СПб. : Питер, 2010. — 256 с.
9. *Дудатьев А.В., Лужецкий В.А., Коротаев Д.О.* Метод оценки информационной устойчивости социотехнических систем в условиях информационной войны // Восточно-Европейский журнал передовых технологий. — 2016. — № 1. — С. 4–11.
10. *Дудатьєв А.В.* Моделі для організації протидії інформаційним атакам // Захист інформації. — 2015. — № 2. — С. 157–162.

Получено 08.08.2016
После доработки 26.09.2016