УДК 681.3

ВЕРОЯТНОСТНАЯ МОДЕЛЬ ОЦЕНКИ ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ

А.В. Гвоздев, И.С. Лебедев, И.А. Зикратов

Описывается вероятностный подход к оценке воздействия сообщений в открытых системах на мнение пользователей. Приводятся основные положения математической теории, пригодной для построения других вероятностных моделей.

Ключевые слова: открытая система, общественное мнение, вероятностная модель, информационное воздействие.

Введение

Современный этап развития информационно-телекоммуникационных систем (ИТКС) характеризуется внедрением новых технологий, повсеместным распространением локальных, корпоративных, глобальных вычислительных сетей. Ведение бизнеса, управление производственным процессом, финансовая и банковская деятельность обусловливают эксплуатацию корпоративных систем с открытым контуром информационной безопасности, где, наряду с использованием закрытых сегментов, необходима обработка, передача, распространение данных и документов в глобальных компьютерных сетях.

Сравнительная легкость доступа к различным страницам, сайтам сети Интернет влечет необходимость идентификации возможных направлений информационного воздействия и атак на ресурсы, находящиеся в открытом доступе [1, 2]. Анализ этих составляющих может являться отправной точкой для определения уязвимостей и обоснования требований к составу и построению средств защиты информации (СЗИ), обрабатывающих текстовую информацию.

Вероятностная модель информационного воздействия

Рассмотрим вычислительную сеть Интернет как глобальную ИТКС. Выделим в ней множество информационных объектов [1, 3]. В нашем случае порталы, сайты, страницы и другие сервисы и ресурсы сети Интернет будут являться информационно-техническими объектами (ИТО). Конечных пользователей, коллективы, анализирующие предоставляемую ИТО информацию, обозначим как информационно-психологические объекты (ИПО). Такой подход позволяет определить модель ИТКС в виде кортежа

$M=<O_t,O_p,T_i,T_o>$,

где O_t – множество информационно-технических объектов; O_p – множество информационно-психологических объектов; T_i – входные информационные потоки текстовой информации; T_o – выходные информационные потоки текстовой информации. Рассмотрим упрощенную структуру анализа воздействия входного информационного потока текстовой информации на ИПО (рис. 1).

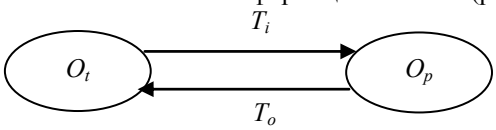

Рис. 1. Информационные потоки ИТКС

Под информационным потоком понимается множество сообщений, получаемых ИПО от объектов противоположного типа (ИТО-ИПО). Использование информационных потоков со стороны злоумышленника подразумевает возможность информационно-психологического воздействия, заключающегося в проведении с применением ИТО комплекса мероприятий по воздействию на интеллектуальную, рационально-волевую, эмоционально-чувствительную сферы психики и подсознание ИПО, направленных на формирование у них прогнозируемых мнений и взглядов, мировоззренческих и психологических установок, поведенческих реакций [4].

Информационно-психологическое воздействие обусловлено угрозами модификации информации и конфиденциальности, осуществляемыми с помощью средств и технологий ИТО [4]. Примером для сети Интернет может служить основанное на модификации информации явление астротерфинга или раскрытие конфиденциальной информации сайтами, подобными Wikileaks. В качестве примера также можно привести подробный отчет об одном эксперименте о влиянии на общественное мнение сайтов, на которых организованы акции астротерфинга [5].

Осуществление угроз связано с организацией потенциально опасных сообщений, содержащих раскрытую конфиденциальную или модифицированную доступную информацию с целью формирования эмоционально-психологической реакции, прямо или косвенно способствующей достижению целей злоумышленника [4]. Ввиду сказанного выше становится актуальным мониторинг и контроль открытых источников. Однако, учитывая их количество и невозможность осуществлять тотальный контроль с применением только «ручных» технологий, возникает задача выбора ИТО, использование которых злоумышленниками может оказать наибольшие негативные последствия, что обусловливает необходимость определения вероятности информационного воздействия, оказываемого информационным сообщением.

Для осуществления информационного воздействия необходимо, чтобы произошла некоторая последовательность событий. Например, пользователь сети Интернет должен выполнить последовательность действий: открыть сайт, на котором злоумышленник поместил информацию, ознакомиться с ней, воспринять сообщение как достоверное.

Разобьем событие ознакомления с содержанием на отдельные составляющие:

- p_1 – вероятность того, что пользователь будет работать с ресурсом, содержащим потенциально опасное информационное сообщение;
- p_2 – вероятность обнаружения (чтения) сообщения;
- p_3 – вероятность оказания воздействия содержания сообщения на конечного пользователя.

Предположим, что вероятность того, что сообщение повлияет на одного пользователя, будет зависеть от вероятностей одновременного наступления указанных выше событий (для простоты будем считать, что эти события независимыми):

$$p_0=p_1\,p_2\,p_3\,. \qquad (1)$$

В общем случае для одного потока текстовой информации выражение (1) при n=3 можно записать следующим образом:

$$p_0=\prod_{i=1}^{n} p_i\,. \qquad (2)$$

Оценивая возможности ознакомления с ресурсами, следует отметить, что среднестатистический пользователь сети Интернет в России, согласно данным, приведенным в [6], регулярно посещает около полутора десятков ресурсов. Пусть ресурс, содержащий потенциально опасное сообщение, просмотрело m независимых пользователей. Тогда считаем, что данный ИТО предоставил m параллельных входных

информационных потоков. Учитывая выражение (2), вероятность информационного воздействия, оказываемого сообщением, можно представить как

$$p = 1 - \prod^{m} (1 - \prod^{n} p_i), \tag{3}$$

где n – количество событий, возникновение которых обусловливает информационное воздействие на пользователя; m – число пользователей, открывших данный ресурс.

Для упрощения, считая равновероятным для каждого пользователя выражение (2), на основе (3) получаем соотношение

$$p = 1 - (1 - p_0)^m .$$

Таким образом, чем больше пользователей ознакомятся с сообщением злоумышленника, тем выше вероятность того, что оно окажет информационное воздействие.

Для наглядного представления характеристик на рис. 2 приведен график для p_0=0,01 (сообщение комментария) и p_0=0,2 (сообщение центральной новости).

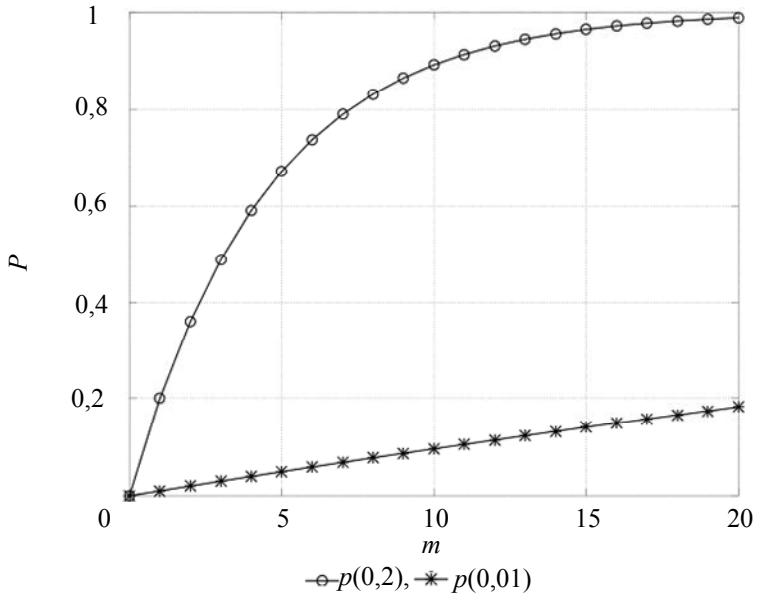

Рис. 2. Вероятность информационного воздействия в зависимости от количества пользователей

Использование ресурса для осуществления информационного воздействия определяет следующее соотношение:

$$\lim p_0 \to 1, \text{ т.е. } \lim p_1 p_2 p_3 \to 1. \tag{4}$$

Для оценки информационного воздействия в упрощенном виде вероятности p_1 и p_3 будем считать зависимыми от индивидуально-психологических особенностей пользователя, на которые структура, ресурсы и состав ИТО не оказывают прямого влияния.

Вероятность события обнаружения p_2 зависит от роли и возможностей лиц, пытающихся воспользоваться ресурсом для оказания информационного воздействия. Если такое лицо является владельцем сайта или занимается его администрированием, то у него существует возможность показать сообщение на наиболее посещаемой странице и обеспечить привлечение к ней аудитории. Если сообщение выставляет рядовой пользователь, то для привлечения к информации он может применять «серые» методы «раскрутки» (частое повторение, организация отдельной темы обсуждения, всевозможное выделение), а также использовать различные пробелы и уязвимости при модерировании ресурса. В связи с этим, в целях достижения максимальной вероятности ознакомления с информацией, в последнее время злоумышленники все чаще применяют различные средства автоматизации и роботов, производящих рассылку сообщений на огромное количество ресурсов.

Вероятность оказания информационного воздействия p_3 определяется стилем и семантикой сообщения. В зависимости от целевой аудитории, на которую ориентировано сообщение, вероятность будет зависеть от структуры, объема и семантического значения информации.

На основе роста количества и частоты сообщений в социальных сетях можно выделить темы, интерес к которым остается неизменным, и события, находящие бурный отклик. Вполне возможно при оценке популярности той или иной темы применять программные средства на основе методов, использующих, например, разные модели сообщения, описанные в [7–10]. Исходя из этого, рассмотрим подход к моделированию возможного сценария атаки с целью осуществления информационного воздействия на пользователей портала сети Интернет.

Модель равномерно-распределенной интенсивности появления сообщений

Пусть каждое сообщение, находящееся на ресурсе, имеет вероятность информационного воздействия p_0 на ИПО. В течение некоторого промежутка времени до модерации сообщение доступно пользователям ресурса. Будем считать, что модерация ресурса происходит постоянно и равномерно. Рассмотрим вероятность информационного воздействия, зависящего от количества потенциально опасных сообщений в единицу времени. Пусть число сообщений n, требующих обработки в единицу времени t, является равномерно-распределенной величиной, т.е.

$$n(t) = \lambda t ,$$

где λ – интенсивность поступления сообщений в единицу времени (единиц/ч), t – промежуток времени с начала наблюдений (ч). Тогда вероятность информационного воздействия на ИПО в течение времени до модерации, когда сообщения остаются на ресурсе, определяется следующим образом:

$$p(t) = 1 - (1 - p_0)^{\lambda t} . \qquad (5)$$

Выражение (5) позволяет провести оценку ИТО с целью выбора объектов мониторинга. На рис. 3 показана зависимость вероятности информационного воздействия при интенсивности появления 10 и 100 сообщений в единицу времени, например, для «центральных» сообщений и комментариев к ресурсу, подобному http://news.mail.ru.

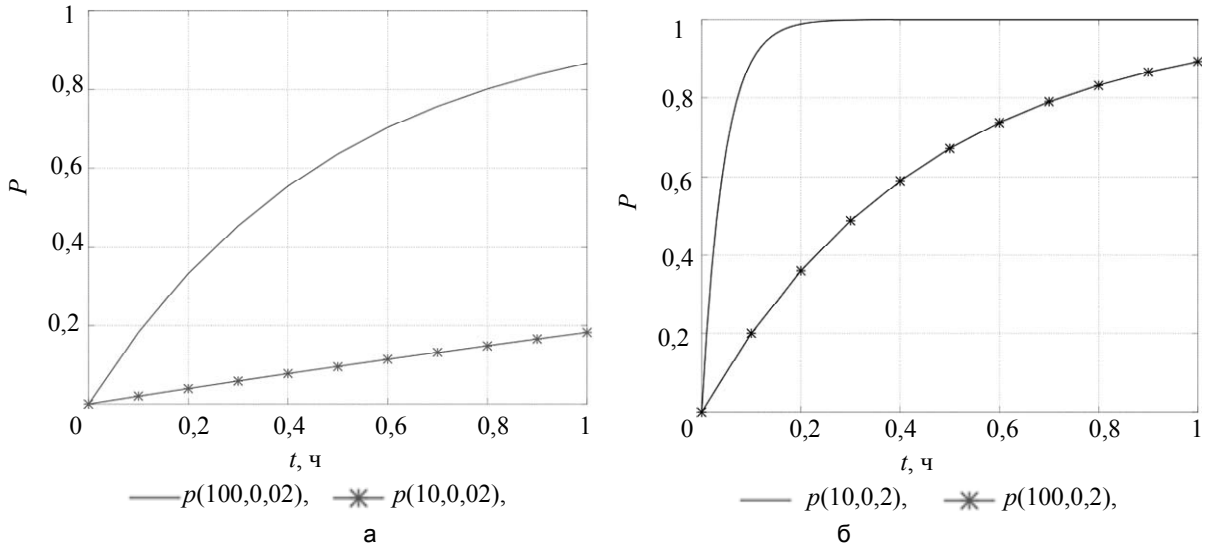

Рис. 3. Зависимость вероятности информационного воздействия при равномерно распределенной величине от вероятности содержания потенциально опасных сообщений p=0,02 (а) и p=0,2 (б) для $\lambda = 100$ и $\lambda = 10$ сообщений/ч

Из приведенных выше зависимостей следует, что чем больше времени не проверяется ресурс, на котором осуществляется публикация текстовых сообщений, тем выше вероятность информационного воздействия, которое и является целью злоумышленника, приведенной в утверждении (4).

Исходя из зависимости (5), становится возможным определить характеристики СЗИ, заключающиеся в частоте модерации ресурса, и вычислить качественные показатели системы автоматического анализа информации, требуемые для обнаружения угроз конфиденциальности и модификации информации. Широко известный ресурс, имеющий большую аудиторию и высокую частоту посещаемости, несет больше потенциальных угроз информационной безопасности.

Заключение

Вероятностная оценка позволяет определить основные направления, где необходимо наращивание сил и средств, обеспечивающих защиту от негативных информационных воздействий. С помощью модели поведения потенциального злоумышленника, стремящегося ознакомить аудиторию с опасными сообщениями, становится возможным имитировать возможные сценарии информационных атак и обосновывать требования к системе защиты информации и мониторинга состояния информационной безопасности.

Работа выполнена в рамках ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2007–2013 годы» по государственному контракту №07.524.12.4009.

Литература

1. Малюк А.А. Современные проблемы защиты информации и пути их решения // Безопасность информационных технологий. – 1999. – № 3. – С. 56–58.
2. Манойло А.В. Информационное противоборство в условиях психологической войны // Закон и право. – 2003. – № 12. – С. 31–34.
3. Дербин Е.А. Информационная безопасность союзного государства как основа его обороноспособности в условиях непрямых действий противника // Вестник Академии военных наук. – 2009. – № 2 (27). – С. 31–38.
4. Тучков Ю.Н. и др. Словарь терминов и определений в области информационной безопасности. – М.: ВАГШ ВС РФ, 2008. – 256 с.
5. Charles H.Cho, Martin L.Martens, Hakkyun Kim and Michelle Rodrigue. Astroturfing Global Warming: It Isn't Always Greener on the Other Side of the Fence // Journal of Business Ethics. – Springer Netherlands, 2011. – V. 104 – № 4. – P. 571–587.
6. Социология Интернета: Методика и практика исследования. – СПб: Ф-т филологии и искусств СПбГУ, 2007. – 130 с.
7. Лебедев И.С. Построение семантически связанных информационных объектов текста // Прикладная информатика. – 2007. – № 3. – С. 23–26.
8. Гвоздев А.В., Лебедев И.С. Адаптированная модель формализации коротких естественно-языковых сообщений для системы мониторинга информационной безопасности открытых вычислительных сетей // Сборник тезисов докладов конференции молодых ученых. Вып. 1. – СПб: СПбГУ ИТМО, 2011. – 295 с.
9. Лебедев И.С., Борисов Ю.Б. Анализ текстовых сообщений в системах мониторинга информационной безопасности // Информационно-управляющие системы. – 2011. – № 2. – С. 37–43.
10. Тузов В.А. Компьютерная семантика русского языка. – СПб: СПбГУ, 2004. – 400 с.

Гвоздев Алексей Вячеславович – Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, аспирант, a.gvozdev@rcwg.net

Лебедев Илья Сергеевич – Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, кандидат технических наук, доцент, info@cit.ifmo.ru

Зикратов Игорь Алексеевич – Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, доктор технических наук, доцент, зав. кафедрой, zikratov@cit.ifmo.ru