АНТИТЕРРОРИСТИЧЕСКИЕ АСПЕКТЫ ПРИМЕНЕНИЯ КОМПЬЮТЕРНОЙ СТЕГАНОГРАФИИ

Л. С. Раткин, *действительный член Международной академии информатизации, к. т. н.*

В Москве, в Выставочном комплексе «Крокус Экспо», с 7 по 10 февраля 2006 года проходил XI Международный форум «Технологии безопасности». Представительный состав участников и широкий спектр практических разработок подтвердили актуальность научных исследований, проводимых ведущими российскими и зарубежными предприятиями, и востребованность продукции в сфере индустрии обеспечения безопасности на внутреннем и внешнем рынках.

Многогранность рассматривавшихся на форуме проблем была отражена в тематике конференций, семинаров и «круглых столов». В частности, были затронуты вопросы применения современных программно-технических средств в антитеррористической деятельности и проведения комплекса организационно-технических мероприятий по профилактике, предварительной диагностике и предотвращению развития нештатных ситуаций.

Практика построения современных систем противодействия террористическим актам предполагает интеграцию посредством мощного телекоммуникационного оборудования перспективных средств наблюдения, контроля и управления доступом, визуализации изображений, идентификации персонала и аутентификации личности. Кроме того, активно применяются комплексы распознавания потенциально опасных лиц на основании ведущихся и регулярно пополняемых соответствующими структурами информационных хранилищ о наиболее важных характеристиках возможных правонарушителей. Доступ к запрашиваемым по сети сведениям не должен замедлять поиск и обработку информации в режиме «реального времени» по базе знаний о подозрительных последовательностях действий (ППД). Эти действия могут быть предпосылками террористических акций, в частности, на объектах повышенной важности (например, энергостанции, больницы) и транспортной инфраструктуры (аэропорты, железнодорожные узлы, федеральные автомагистрали и др.).

Мониторинг развивающихся ППД в автоматическом и автоматизированном режимах должен сопровождаться классификацией ситуаций по степени угроз, выбором критерия оптимизации в каждой конкретной ситуации и выработкой рекомендаций группе операторов в сети диспетчерских пунктов.

Следует отметить, что в настоящее время компьютерная стеганография (КС) как наука переживает очень важный этап становления. Назрела острая необходимость в разработке инновационных механизмов обеспечения безопасности информации для систем защиты данных. Вместе с тем научный потенциал КС-методов, которые уже разработаны или еще разрабатываются, оценен весьма приблизительно (и, на наш взгляд, недостаточно полно). Многие направления НИР и ОКР только начинают рассматриваться в качестве перспективных для практической реализации КС (их финансирование пока осуществляется за счет собственных средств научных и производственных предприятий и личных средств разработчиков). Поэтому преимущественное развитие получают такие области КС-знаний, экономический эффект от использования которых очевиден. К числу активных сфер применения КС можно отнести антитерроризм. Учитывая, что компьютерная стеганография является обоюдоострым оружием (то есть способна нанести значительный ущерб при защите и нападении), необходим анализ не только оборонительных, но и наступательных КС-стратегий.

Примером применения КС в террористической деятельности [1] может стать, в частности, размещение на странице интернет-сайта любого материала (например, серии графических или текстовых файлов), в каждый из которых, как в файл-контейнер, в соответствии с используемым форматом будет вложено особое сообщение (или его фрагмент) [2]. Прочитать его можно будет, располагая точными

данными о местонахождении стегоконтейнеров (так называемых «внешних» адресах), порядке их открытия и сведений о «внутренних» адресах, по которым в каждом контейнере располагается «информационная закладка» [3]. Неточность в любом адресе приводит к ошибке в процедуре чтения сообщения и, соответственно, к некорректному выполнению содержащихся в нем инструкций (например, террористического характера). Учитывая многообразие файловых форматов и множество методов сокрытия данных в файлах различных групп, объем работ специалистов-экспертов по выявлению «информационных закладок» и проверке их содержимого на предмет террористической угрозы многократно возрастает. Это предполагает привлечение аппарата КС для разработки спецсредств ревизии интернет-ресурсов.

Рассмотренная наступательная КС-стратегия является по своему характеру статической. Угроза от ее реализации может быть достаточно существенной, если в сообщении-закладке размером несколько десятков байт, распределенных по большой группе контейнеров, скрывается сообщение высокой степени важности (например, об обороноспособности или степени боеготовности конкретного государственного объекта). Но при условии неизменности текста сообщения («информационной закладки») соответствующий риск многократно возрастает при применении динамической КС-стратегии. В этом случае предполагается регулярное (с произвольным временным интервалом) изменение местонахождения каждого файла-контейнера (или замена контейнера на идентичный, имеющий близкий к исходному размер с задаваемой заранее точностью), в каждом из которых заложен стегоквант (порция скрываемой информации). Предельной возможностью рассматриваемой динамической наступательной КС-стратегии является быстрая смена размеров стегоквантов, внутренних (то есть находящихся внутри каждого стегоконтейнера) и внешних (самих стегоконтейнеров) адресов, что значительно затруднит поиск и распознавание скрываемого текста сообщения и, соответственно, воспрепятствует быстрой адекватной реакции на угрозу, содержащуюся в сообщении.

Какие же оборонительные КС-стратегии могут быть противопоставлены столь изощренным информационным инструментам? Прежде всего, распознаваемые КС-средства и методы наступательного характера должны пополнять базу знаний, и процесс самообучения комплекса должен происходить преимущественно в автоматизированном режиме. Кроме того, оборонительным КС-системам свойственна контригра, то есть после определения текста сообщения производится его предварительно согласованная замена с информированием соответствующих органов об исходном сообщении, подставленном вместо него тексте и времени проведения подстановки. Наконец, спецсредства ревизии интернет-ресурсов должны работать «на опережение» террористических угроз (ТУ), а именно:

- регулярно обрабатывать (просматривать) определенные информационные массивы;
- сохранять данные о наиболее важных характеристиках потенциальных стеганографических контейнеров;
- производить сравнение изменений характеристик и при обнаружении несоответствий передавать данные на более детальное исследование с помощью специальных инструментов и процедур.

Отметим, что при современном уровне развития информационных и телекоммуникационных технологий для сокрытия факта работы спецсредств в среде интернет-ресурсов возможна их успешная интеграция в поисковые системы (Yandex, Rambler, Google и др.), а также встраивание элементов эвристического анализа потенциальных стегоконтейнеров в действующие механизмы индексации массивов данных.

Примером использования современных оборонительных КС-стратегий для борьбы с терроризмом также является разработка операционных систем (ОС) нового поколения, защищенных от атак извне по сети благодаря принципиально новым механизмам надежности вычислений и безопасности обработки данных. Например, известно о дорабатываемом фирмой «Microsoft» ядре ОС, состоящем из более чем 300 000 строк программного кода на языке C#. Одной из особенностей создаваемой ОС, получившей проектное название Singularity, является использование технологии программного изолирования процессов (в оригинале – Software Isolated Processes), при которой каждый из запускаемых изолированных процессов (ИП) выполняется скрытно, в отдельном «контейнере», не доступном из других ИП. При взломе одного из ИП (например, программы мониторинга ресурсов персонального компьютера или всей сети) доступ к другому ИП (например, копирования файла или обработки запроса к базе данных) и его характеристикам обычным способом получить будет нельзя, поскольку данные о параметрах хранятся «внутри» каждого ИП [4].

ВЫВОДЫ

Современные террористические угрозы предполагают повышение уровня безопасности всего спектра программно-технических средств. Создание ОС нового поколения на основе анализа оборонительных и наступательных КС-стратегий способно минимизировать риски от скрытого доступа к данным на ПЭВМ по сети.

В настоящее время актуальной задачей является разработка специализированных стеганографических программных комплексов (ССПК), осуществляющих ревизию интернет-ресурсов. Функционирование ССПК в непрерывном режиме обеспечит поиск скрытых информационных закладок и проверку их содержимого на наличие ТУ.

Помимо интернет-ресурсов и ОС, компьютерная стеганография активно применяется в промышленных информационных системах. Использование КС при проектировании стегорепозиториев будет рассмотрено в следующей публикации.

ЛИТЕРАТУРА

Черняк Л. Стеганография и террор // Открытые системы. – 2002. – № 7–8. – С. 59–61.

Рэдклифф Д. Стеганография: скрытые данные // COMPUTER WORLD Россия. – 2002. – 10 сентября. – С. 28.

Байерс С. Утечка данных через скрытые тексты в опубликованных документах // Открытые системы. – 2004. – № 5. – С. 53–56.

Microsoft разрабатывает новую защищенную ОС // Хакер. – 2005. – № 12 (84). – С. 6.