Таким образом, в итоге можно сделать следующие выводы.

1. Анализ необходимого энергетического потенциала и эффективности средств РЭП свидетельствует о наибольшей уязвимости СРНС от воздействия имитирующих помех.

2. Предложено выражение

$$P_{\text{ПЗ}} = P_{\text{РНЗ0}} + \left(\frac{p_c (A_{cc} - m(k+1))! m!}{(A_{cc} - mk)!} + \sum_{i=1}^{n-1} P_{Pзi} p_i \right) \times$$

$$\times P_{ИСП} P_{ПП} \left(P_{РНЗ1} - P_{РНЗ0} \right),$$

которое, в отличие от известных, позволяет оценить помехозащищенность СРНС в условиях стохастического применения ей НС с учетом снижения априорной неопределенности параметров НС в процессе функционирования системы РЭП.

Литература

1. Global Navigation Space Systems: reliance and vulnerabilities // Report of The Royal Academy of Engineering. London: March, 2011. – 48 p.
2. Дятлов А.П., Кульбикаян Б.Х. Радиомониторинг излучений спутниковых радионавигационных систем. М.: Радио и связь, 2006. – 270 с.
3. Борисов В.И., Зинчук В.М. Помехозащищенность систем радиосвязи. Вероятностно-временной подход. М.: РадиоСофт, 2008. – 260 с.
4. Дятлов А.П., Дятлов П.А., Кульбикаян Б.Х. Радиоэлектронная борьба со спутниковыми радионавигационными системами. М.: Радио и связь, 2004. – 226 с.
5. Основы теории скрытности. Под ред. З.М. Каневского. Воронеж: Изд. ВГУ, 2006. – 197 с.

ABOUT THE NOISE IMMUNITY EVALUATION OF SATELLITE RADIO NAVIGATION SYSTEMS

Zhuk A.P., Orel D.V.

This work introduces the way to evaluate the noise immunity of satellite radio navigation systems with high structural secrecy of navigation signals by using the expression, that takes into account the reduction of prior uncertainty parameters of navigation signals during the jamming complex system works.

Keywords: *noise immunity, satellite radio navigation, structural secrecy, simulating interference, radio electronic strike.*

Жук Александр Павлович, к.т.н., профессор Кафедры «Организация и технологии защиты информации» (ОТЗИ) Ставропольского государственного университета (СтавГУ). Тел. (8-652) 35-74-09; 8-918-884-14-81. E-mail: alekszhuk@mail.ru

Орел Дмитрий Викторович, ассистент Кафедры ОТЗИ СтавГУ. Тел. (8-652) 95-56-36; 8-918-740-11-74. E-mail: kde.def@gmail.com

УДК 004.056

ПРИНЦИПЫ МНОГОУРОВНЕВОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Алексеев А.П., Макаров М.И.

Рассмотрены принципы защиты информации, основанные на создании нескольких барьеров: криптографического, стеганографического, алгоритмического и пространственно-временного распыления.

Ключевые слова: защита информации, криптография, стеганография, барьеры, пространственно-временное распыление информации.

Введение

Защита передаваемой и хранимой информации в настоящее время базируется на принципах, фундаментально разработанных в криптографии и стеганографии. С помощью криптографических методов защищаемое сообщение преобразуется в набор символов, нечитаемый без ключа [1]. Приемы стеганографии позволяют создать скрытый канал связи, который сложно обнаружить даже с помощью специальных методов обработки информации [2].

Специалистами проведено большое число результативных криптографических атак на известные шифры [3] и на стеганографические методы защиты [2]. Наличие успешно проведенных атак говорит об имеющейся уязвимости существующих принципов защиты информации.

Процесс разработки средств защиты информации и средств атаки на шифры и методы сокрытия сообщений носит соревновательный (итерационный) характер. Как правило, через несколько лет после создания широко распространенного шифра появляется эффек-

тивная атака на этот шифр, и его использование постепенно затухает. Мозговой штурм по разработке новых алгоритмов защиты стимулируется проведением международных конкурсов [3].

Пространственное распыление сообщения

Принципиально новым подходом к защите информации может стать метод формирования нескольких уровней защиты сообщений (см. рис. 1). Под сообщением будем понимать любую передаваемую (хранимую) информацию или данные. Одним из дополнительных барьеров защиты (помимо криптографического и стеганографического) может стать пространственное распыление защищаемой информации [5].

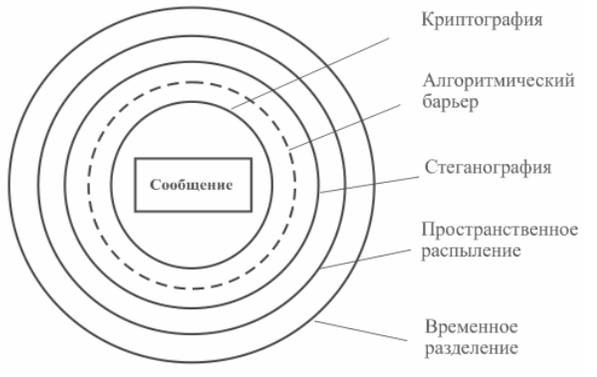

Рис. 1. Барьеры защиты сообщения

Основная идея пространственного распыления информации состоит в том, что сообщение дробят на возможно мелкие составляющие (предложения, слова, символы, блоки символов, группы байт, байты, группы бит, биты) и передают частями, распределяя их по нескольким каналам связи $(K_1 ... K_n)$.

Перехват нарушителем С (см. рис. 2) всех составляющих сообщения осложняется тем, что у корреспондентов А и В есть возможность использования нескольких доступных им телекоммуникационных каналов (радио, спутниковые, проводные, кабельные, радиорелейные).

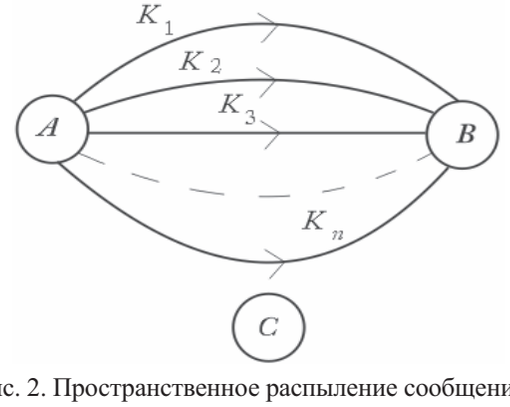

Рис. 2. Пространственное распыление сообщения

Передача информации в глобальных сетях возможна с помощью множества существующих услуг (электронная почта, мессенджеры, чаты, форумы, блоги, распределенные базы данных WWW и т.п.). Использование сотовой связи позволяет распылить сообщение по нескольким MMS или SMS и передать их с помощью большого числа телефонных каналов.

Временное разделение сообщения

Помимо трех перечисленных уровней защиты передаваемой информации можно создать еще один уровень (четвертый), который технически и алгоритмически гармонично сочетается с ранее рассмотренными барьерами. Это – временное разделение сообщения (передача данных по заранее согласованному расписанию) [6].

Пространственное и временное разделение сообщения удачно сочетаются между собой, дополняя друг друга. Эти два барьера можно представлять в виде единого барьера и назвать его пространственно-временным распылением сообщения. Идею пространственно-временного распыления сообщения иллюстрирует рис. 3.

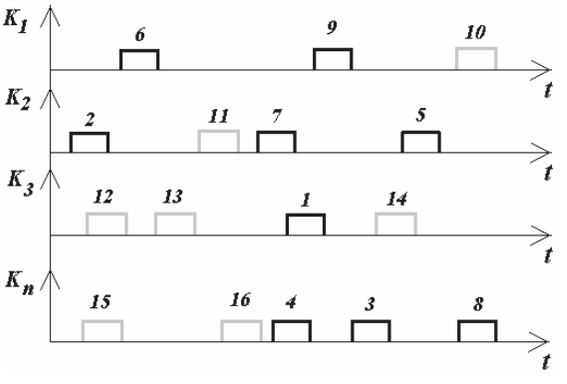

Рис. 3. Пространственно-временное распыление сообщения

Информационные блоки 1…9, содержащие транслируемое сообщение, передаются в псевдослучайном порядке по каналам связи $(K_1 ... K_n)$. Моменты передачи блоков сообщения также является псевдослучайными. Передача информационных блоков перемежается посылкой маскирующих (дезинформирующих) блоков 10…16. Порядок трансляции блоков, номера каналов и временные окна устанавливают с помощью секретного ключа. Заметим, что если для связи используется только один телекоммуникационный канал, то пространственно-временной барьер превращается во временной барьер.

Пятый (алгоритмический) барьер базируется на таком способе обработки передаваемых блоков

криптограммы, при котором отсутствие хотя бы одного перехваченного блока вызывает у криптоаналитика труднопреодолимые вычислительные сложности. Ближе всего по идеологии (по замыслу и использованию) к этому барьеру находятся режимы шифрования, которые описаны в отечественном стандарте ГОСТ 28147-89, американском стандарте DES [7] и публикациях [1; 4]. Пятый барьер как бы является продолжением криптографического барьера, однако методологически его целесообразно выделить в отдельный уровень защиты.

Таким образом, путем создания множества барьеров разного вида можно осуществить принцип комплексной, многоуровневой защиты информации. В каждом конкретном случае стороны обоснованно выбирают достаточную степень защищенности сообщения (число используемых барьеров, вид шифра, длину ключа, виды стеганографических контейнеров, способы стеганографического внедрения информации в контейнеры, вид и число используемых каналов связи или носителей хранения информации, количество временных окон для передачи информации).

Ясно, что реализация предлагаемых мер повышения криптостойкости сопровождается увеличением времени передачи сообщения, числа ошибок при передаче сообщения, усложняет процедуру передачи, снижает удобство хранения информации. Регулировать степень защиты сообщения (значит, и варьировать время передачи сообщения, изменять сервисные свойства) можно путем выборочного использования не всех барьеров, а только достаточной их части. Оперативная передача информации (когда ценность информации исчисляется часами и даже минутами) может происходить при минимальном числе используемых барьеров.

Рассмотрим подробнее идею временного разделения передаваемых сообщений.

Сообщение дробят на блоки, которые вначале шифруют, а затем стеганографически внедряют в отдельные контейнеры. Передача стегоконтейнеров происходит по множеству каналов связи (тем самым осуществляется распыление информации в пространстве). Так формируются три внутренних барьера защиты, показанных на рис.1 сплошными линиями.

Для создания четвертого барьера защиты информации блоки сообщений передают по каналам связи в псевдослучайные моменты времени, причем для уменьшения вероятности перехвата продолжительность передачи фрагмента сообщения устанавливают минимально возможной, но достаточной для принимающей стороны. Расписание передачи информации (временные окна) определяется корреспондентами с помощью ключа. Передачу информационных блоков в канале связи перемежают трансляцией информационно пустых (маскирующих) блоков.

Идею передачи информации по расписанию рассмотрим на примере использования для связи глобальной сети Internet. Программную реализацию принципа временного разделения сообщения можно осуществить с помощью различных языков программирования (JavaScript, Perl, PHP, Java и т.д.).

Рассмотрим, как создать четвертый барьер защиты информации с помощью языка программирования JavaScript. Приведенный ниже скрипт позволяет кратковременно заменять фотографию const.jpg на фотографию secret.jpg. В данном случае замена будет происходить в 17 ч. 18 мин. 35 С, а обратная замена - в 17 ч. 19 мин. 26 С. Передаваемое сообщение предварительно скрыто размещают в контейнере secret.jpg.

```
<script language="JavaScript">
var start = new Date();
var end = new Date();
start.setHours(17);
start.setMinutes(18);
start.setSeconds(35);
end.setHours(17);
end.setMinutes(19);
end.setSeconds(26);
var now = new Date();
st = start.getTime();
et = end.getTime();
time = now.getTime();
if ((time >= st) && (time < et))
document.write("<img src=\"secret.jpg\">");
else document.write("<img src=\"const.jpg\"
>");
</script>
```

В рассмотренном примере демонстрация секретной информации на Web-странице происходит в течение короткого времени. Внешне две демонстрируемые фотографии должны быть одинаковыми (объекты-близнецы). Однако фотография secret.jpg является стегоконтейнером и содержит в себе скрытую информацию.

Приведенный пример лишь иллюстрирует идею временного распыления информации, но такую реализацию нельзя использовать на практике. Недостатком подобной защиты сообщения является имеющаяся у криптоаналитика возможность ознакомления с кодом скрипта, за счет чего

он в состоянии определить момент демонстрации (передачи) стегоконтейнера. Просмотр текста программы осуществляется стандартным путем с помощью любого браузера. Этот недостаток присущ всем скриптам, исполняемым на клиентской ЭВМ. Однако даже при имеющейся возможности по коду скрипта установить время подмены контейнеров у криптоаналитика остается нерешенной задача определения доменного адреса (IP-адреса) Web-страницы, на которой размещен стегоконтейнер. Доменные адреса используемых Web-страниц известны только корреспондентам. Выбор корреспондентами используемых серверов и Web-страниц (каналов связи) осуществляется с помощью ключа.

Рассмотрим пример реализации этой же идеи с помощью языка программирования PHP. Следующий скрипт заменяет в 10 ч. 47 мин. Web-страницу page2.html страницей page1.html, которая является стегоконтейнером. Через 1 мин. происходит обратная замена.

```
<?php
// формат ччмм
//Установка времени начала демонстрации стегоконтейнера
$start_time = '1047';
//Установка времени конца демонстрации стегоконтейнера
$end_time = '1048';
//Считывание текущего времени
$now_time = date('Gi');
//Сравнение текущего времени с моментами начала и конца демонстрации
if ($now_time >=$start_time && $now_time <$end_time) {
//Загрузка страницы, содержащей скрытые данные
header('location:page1.html');
exit;
}
else {
//Загрузка маскирующей страницы
header('location:page2.html');
exit;
}
?>
```

Повышение криптостойкости в результате применения принципа временного разделения сообщения происходит за счет того, что за определенное время может осуществляться многократная подмена оригинального объекта различными объектами-близнецами, но только контейнер, переданный в заранее обусловленное время, содержит полезную для получателя информацию. При этом маскирующие объекты-близнецы могут содержать дезинформацию (вложение в контейнере есть, но оно не относится к передаваемому сообщению).

Рассмотренный принцип легко развить и усовершенствовать, например, можно на одной Web-странице сразу демонстрировать несколько стегоконтейнеров (рисунки, тексты, фотографии, видео) и передавать не один блок информации за определенный промежуток времени, а несколько. Другими словами: пространственно-временное распыление информации можно вести не только по каналам связи, но и по контейнерам. При этом блоки разных сообщений целесообразно переставлять и передавать их не последовательно, а в псевдослучайном порядке. Это повышает вычислительную сложность криптоанализа.

Скрипты, написанные на языке PHP, являются серверными приложениями, поэтому криптоаналитик не может самостоятельно получить листинги программ и на основе анализа кода определить, в какое время происходит подмена объекта. Обнаружить подмену можно по изменяющемуся содержимому контейнера, но для этого придется непрерывно контролировать множество Web-страниц. Сложность пеленгации Web-страницы состоит еще и в том, что доменный адрес криптоаналитику неизвестен, а до момента обнаружения роботом поисковой системы нового доменного адреса проходит несколько дней.

Технологически надежно реализовать непрерывный мониторинг большого числа Web-страниц сложно. Это требует от криптоаналитика существенных капитальных и эксплуатационных вложений. Таким образом, четвертый барьер – это технологический барьер, сложность преодоления которого состоит в необходимости непрерывного контроля множества Web-страниц, для чего требуется использование аппаратных средств большой мощности.

Алгоритмический барьер

Алгоритмический барьер защиты (пятый уровень защиты) в принципе может быть включен в криптографический барьер. Однако его целесообразно выделить особо, как это сделано в стандартах шифрования. Этот бастион защиты базируется на такой последовательности обработки блоков, при которой отсутствие даже одного блока криптограммы приводит к необходимости решения вычислительно сложной задачи.

Реализовать указанную идею можно следующим образом. Предположим, что для сцепления

блоков используется режим шифрования CBC (Cipher-Block Chaining) шифра DES [7], сцепление в котором происходит в соответствии с выражением:

$$C_i = E_k(M_i \oplus C_{i-1}), \quad (1)$$

где C_i – очередной блок криптограммы; k – ключ шифрования; E_k – шифрующее преобразование на ключе k; M_i – очередной блок открытого текста; C_0 – вектор инициализации (псевдослучайный вектор); $\oplus$ – логическая операция «Исключающее ИЛИ». Из (1) видно, что отсутствие блока C_{i-1} делает невозможным расшифрование следующего блока C_i. Однако все остальные блоки шифрограммы будут расшифрованы штатно.

Сцепление блоков криптограммы можно осуществить иначе [4]:

$$C_i = E_k(M_i \oplus C_{i-1} \oplus C_{i-2} \oplus ... \oplus C_0). \quad (2)$$

При отсутствии блока C_t невозможно расшифровать блоки с индексами $i \geq t+1$. Тем не менее дешифрация блоков с меньшими порядковыми номерами возможна.

Итак, режим сцепления блоков (2) имеет недостаток: отсутствие на приеме нескольких блоков все же позволяет получить часть открытого текста (точнее: частично преодолеть алгоритмический барьер). Для устранения этого недостатка предлагается шифрующее преобразование (2) выполнить повторно, причем при втором шифровании блоки криптограммы, полученные после первого шифрования, зеркально переставить местами (первый – последний, второй – предпоследний т.д.):

$$P_1 = C_m, P_2 = C_{m-1}, ..., P_{m-1} = C_2, P_m = C_1.$$

Новая последовательность блоков повторно шифруется по алгоритму (2):

$$Z_i = E_k(P_i \oplus Z_0 \oplus Z_1 \oplus ... \oplus Z_{i-2} \oplus Z_{i-1}).$$

Такой алгоритм обработки информации делает зависимым каждый блок формируемой криптограммы от всех ее блоков (происходит полное сцепление всех блоков).

Анализируя рис. 1, можно отметить, что первый бастион защиты информации (криптографический) держится на вычислительной сложности перебора всех имеющихся криптографических ключей. Для преодоления второго барьера (стеганографического) криптоаналитикам требуется вести постоянный анализ множества контейнеров разного вида (звуковых, графических, видеофайлов, архивов, баз данных, HTML-страниц) с целью обнаружения в них скрытых вложений.

Преодоление третьего барьера (пространственное распыление) предполагает пеленгацию всех телекоммуникационных каналов, существующих между корреспондентами. При этом криптоаналитику необходимо отделить камуфлирующие каналы от информационных каналов. Этот барьер базируется на технической сложности реализации пеленгующей аппаратуры.

Для взлома четвертого барьера (временное разделение) нужен круглосуточный мониторинг обнаруженного канала связи. Причем по одному каналу связи могут передаваться фрагменты разных сообщений, перемешанных во времени. Передача информационных контейнеров может перемежаться передачей камуфлирующих контейнеров.

Пятый уровень защиты (алгоритмический), как и первый, опирается на вычислительную сложность решения задачи. Легко заметить, что каждый последующий уровень защиты (см. рис. 1) охватывает (инкапсулирует) предыдущие уровни защиты. Доступ к внутренним барьерам невозможен без преодоления внешних уровней защиты обнаруженного канала связи.

Заключение

Основные принципы многоуровневой защиты информации заключаются в следующем. Сообщение шифруют с помощью блочного шифра. Осуществляют полное алгоритмическое сцепление всех блоков криптограммы, то есть содержимое каждого блока криптограммы делают зависимым от содержимого других блоков. Зашифрованные блоки стеганографически внедряют в контейнеры различных форматов. Контейнеры пересылают по множеству каналов связи разного вида в секретные моменты времени (осуществляют пространственно-временное распыление информации).

Реализация принципа пространственно-временного распыления основывается на создании нескольких объектов-близнецов, среди которых только часть объектов содержит скрытую информацию, а остальные объекты являются маскирующими.

Литература

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: ТРИУМФ, 2002. – 816 с.

2. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. М.: СОЛОН-Пресс, 2002. – 272 с.
3. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. СПб.: БХВ-Петербург, 2009. – 576 с.
4. Фомичев В.М. Методы дискретной математики в криптологии. М.: Диалог_МИФИ. 2010. – 424 с.
5. Алексеев А.П., Орлов В.В. Сокрытие сообщений путем их распыления в пространстве // ИКТ. Т.6, №3, 2008. – С. 52-56.
6. Алексеев А.П. Метод пространственно-временного распределения информации // Тезисы XVI РНТК ПГУТИ. Самара, 2009. – С. 167-168.
7. Data Encryption Standard (DES). Federal Information Processing Standards (FIPS). Publication 46-3. 25.10.1999. – 22 p.

PRINCIPLES OF MULTILEVEL PROTECTION OF THE INFORMATION

Alekseev A.P., Makarov M.I.

Principles of protection the information based on creation of several barriers are considered: cryptographic, steganographic, algorithmic and existential dispersion.

Keywords: *protection of the information, cryptography, steganography, barriers, existential dispersion of the information.*

Алексеев Александр Петрович, к.т.н., доцент Кафедры «Информатика и вычислительная техника» (ИВТ) Поволжского государственного университета телекоммуникаций и информатики (ПГУТИ). Тел. (8-846) 262-97-46. E-mail: apa2008@rambler.ru, apa@bk.ru

Макаров Максим Игоревич, ассистент кафедры ИВТ, ПГУТИ.). Тел. (8-846) 228-00-59. E-mail: moox700@gmail.com

УДК 621.396.677; 621.397.671

ПРОСТРАНСТВЕННО-ЧАСТОТНЫЕ ХАРАКТЕРИСТИКИ ЭЛЕКТРОМАГНИТНОГО ВОЗБУЖДЕНИЯ КОМПЛЕКСА СЛУЧАЙНЫХ АНТЕНН

Заседателева П.С., Маслов О.Н.

Рассматриваются пространственно-частотные характеристики электромагнитного излучения (ЭМИ) в многоэтажном здании, где размещен комплекс сосредоточенных и распределенных случайных антенн (СА и РСА). Представлены результаты экспериментальных измерений, которые являются исходными данными для исследования многоканальных СА и РСА методом статистического имитационного моделирования (СИМ) и проектирования систем защиты конфиденциальной информации (КИ).

Ключевые слова: защита конфиденциальной информации, многоканальные случайные антенны, способы электромагнитного возбуждения, метод статистического имитационного моделирования, исходные данные.

Введение

В многоэтажном здании, расположенном в мегаполисе, сегодня размещается целый комплекс устройств, соответствующих определению СА и РСА [1-3]:

- сосредоточенные многоканальные СА в виде малогабаритных радиоэлектронных (РЭС) и других технических средств (абонентские терминалы, базовые станции и концентраторы систем сотовой связи и широкополосного радиодоступа; портативные радиостанции; оконечные устройства систем связи и сигнализации; блоки ЭВМ; экранированные камеры и корпуса аппаратуры; датчики систем охраны и управления; бытовая радиоэлектронная аппаратура; офисное оборудование и т.п.);
- многоканальные РСА в виде отдельных проводных линий связи в составе компьютерных и других сетей различного назначения;
- разветвленные РСА в виде систем проводов электропитания и заземления аппаратуры, оборудования оповещения и сигнализации;
- разветвленные РСА в виде систем металлических и металлопластиковых труб водоснабжения и центрального отопления;