

Труды XX научной конференции по радиофизике,  
посвященной 110-летию со дня рождения Г.С. Горелика

**Секция  
«Информационные системы.  
Средства, технологии, безопасность»**

*Председатель  
кандидат технических наук, доцент  
Леонид Юрьевич Ротков*

## ОБЛАСТЬ ПРИМЕНЕНИЯ СТЕГАНОГРАФИИ

А.А. Горбунов, А.Г. Леонова

ННГУ им. Н.И. Лобачевского

Стеганография изучает способы сокрытия конфиденциальных данных [1]. Основной чертой методов стеганографии является встраивание секретного сообщения в «непримечательный» объект, который затем открыто передаётся адресату. При этом ни у кого из посторонних не возникает мысли, что за обычным сообщением скрывается другое.

Криптография изменяет вид информации так, что её смысл становится недоступным для непосвящённых. Наличие зашифрованного сообщения уже привлекает внимание непосвящённой стороны. Стеганография скрывает факт передачи тайной информации.

Основные направления цифровой стеганографии соответствуют следующим практическим задачам [2]:

1. скрытая передача информации;
2. встраивание цифровых водяных знаков (ЦВЗ);
3. встраивание идентификационных номеров.

Базовым понятием стеганографии является контейнер – сообщение (файл), в которое встраивается скрываемая информация.

Важным условием качества стеганографии является неотличимость по внешним признакам пустого контейнера, заполненного контейнера и частично заполненного контейнера. Этим условием определяется специфика областей данных контейнера, куда помещаются биты скрываемого сообщения. Особую важность это условие приобретает при встраивании сообщения в контейнер, уже содержащий ЦВЗ [2].

Рассмотрим особенности разных видов контейнеров.

Специфика контейнера - текстового файла такова, что символы текста не должны изменяться. Есть два основных стеганографических метода, которые здесь можно применить:

- если адресант имеет дело с электронным экземпляром текстового файла, то информацию можно встраивать, изменяя параметры табуляции (например, при использовании пропорциональных шрифтов на глаз нельзя отличить, поставлен 1 или 2 знака «пробел»);
- если текстовый файл недоступен для изменения, но адресант и адресат имеют его копии, то можно составить ключ, указывающий на значимые символы в тексте, и задача сводится к передаче ключа, также осуществляемой различными способами, в т.ч. стеганографическими.

Ёмкость текстовых контейнеров относительно мала.

Более интересным с точки зрения стеганографии является контейнер - растровое изображение. В нём цвет каждой точки кодируется целым числом байт, значение которых соответствует линейной шкале интенсивности цветовой составляю-

щей. То есть, разряды (биты) имеют различный вес, и изменение младшего бита приводит к изменению цветового оттенка точки, не воспринимаемому глазом человека. Если заменить младшие разряды битами скрываемого сообщения, то изображение для восприятия человека останется неизменным. Если один пиксель кодировать тремя байтами, отвечающими за глубину красной, зелёной и синей составляющих (RGB), то в одном пикселе скроются три бита информации.

Наибольшей ёмкостью обладает контейнер - видеофайл. Глаз человека при смене кадров с частотой 16 Гц и выше не различает отдельные кадры – они сливаются в движущееся изображение. Поэтому изменение оттенков точки в динамике менее заметно глазу, чем в статичном изображении. Контейнер сам по себе очень объёмный и позволяет скрывать больший объём информации, чем изображение или текст.

В рассмотренных случаях можно представить контейнеры как массивы разной мерности:

- текстовый контейнер – одномерный массив;
- изображение – двумерный массив;
- видео – трёхмерный массив.

Скрытие информации большей мерности в контейнере меньшей мерности не используется (это не всегда возможно, и даже если в конкретном случае это удалось, то размер файла-контейнера превысит стандартный, что привлечёт к нему внимание). Выгодно скрывать сообщение меньшей мерности в контейнере большей мерности.

Если  $A = (a_{i_1, i_2, i_3, \dots, i_n})$  – пустой контейнер, а  $B = (b_{i_1, i_2, i_3, \dots, i_n})$  – контейнер со стеганографическим вложением, то критерием качества стеганографии можно считать:

$$\left| a_{i_1, i_2, i_3, \dots, i_n} - b_{i_1, i_2, i_3, \dots, i_n} \right| < p ,$$

где  $p$  – порог сенсорного разрешения органа чувств человека.

В работе рассмотрены общие методы и понятия стеганографии. В частных случаях использования стеганографических методов предметом изысканий являются дополнительные специфические понятия и критерии.

- [1] Компьютерная стеганография: теория и практика. /Г.Ф. Конахович, А.Ю. Пузыренко. – Киев: МК-пресс, 2006.
- [2] Цифровая стеганография. /В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: Солон-пресс, 2009.

## СРАВНЕНИЕ ПРОТОКОЛОВ IKE

А.В. Деребенец, А.А. Рябов

ННГУ им. Н.И. Лобачевского

Виртуальные частные сети (ВЧС) используются организациями для соединения с удаленными сайтами и с другими организациями. ВЧС используют каналы связи, арендованные у телекоммуникационных провайдеров. ВЧС обладают следующими свойствами:

- обеспечение конфиденциальности передаваемой информации за счет ее шифрования;
- обеспечение аутентификации участников взаимодействия;
- прозрачны для протоколов более высоких уровней.

Наиболее распространены ВЧС на базе протокола IPSec. Основной составляющей IPSec, решающей задачи управления ключами и аутентификации, является протокол Internet Key Exchange (IKE). В настоящее время наиболее часто используется IKEv1.

Взаимодействие по протоколу IKEv1 происходит в 2 фазы [1]. На первой фазе происходит аутентификация взаимодействующих сторон и создается безопасный канал между ними. На второй фазе созданный в первой фазе безопасный канал используется для обмена ключами, согласования общей политики безопасности, установления ассоциаций безопасности IPSec.

Рассмотрим подробнее первую фазу IKEv1. Фаза 1 может проходить в одном из двух режимов: основном и агрессивном. В основном режиме используется 3 процедуры:

- согласуются алгоритмы и правила обмена;
- обмен открытой информацией с использованием протокола Диффи-Хеллмана;
- установление защищенного канала связи.

Агрессивный режим обходится меньшим числом процедур.

Для примера, с помощью виртуальных машин создана сеть ВЧС. Эксперимент проводился с использованием агрессивного режима фазы 1 и аутентификации удаленного доступа с разделяемым ключом. В ходе эксперимента уязвимость протокола, выражаясь в передаче хэш-образа пароля доступа в незашифрованном виде, подтвердилась. Данная уязвимость позволяет злоумышленнику подключаться к VPN-шлюзу в качестве легального пользователя.

В ходе эксперимента произведено измерение производительности VPN-сети при различных режимах протокола IKEv1. Использование агрессивного режима фазы 1 IKEv1 позволяет увеличить производительность соединения почти в 2 раза.

Новая версия протокола IKE устраняет недостатки первой версии. В IKEv2 нет агрессивного и основного режимов. Увеличена производительность за счет меньшего числа обменов информацией. Кроме того в IKEv2 предусмотрен механизм защиты от DoS атак [2].

Показанная в работе уязвимость IKEv1 в IKEv2 отсутствуют.

Несмотря на уязвимость, применение агрессивного режима фазы 1 IKEv1 целесообразно, т.к. этот режим показал лучшие показатели производительности сети. Другие механизмы аутентификации клиента, основанные на методе открытого ключа делают рассмотренную атаку невозможной. Возможно применение метода разделяемого ключа, если вероятность прослушивания канала равна нулю (все коммуникации находятся в пределах контролируемой зоны).

В дальнейшем планируется измерение производительности протокола IKEv2.

- [1] Кульгин М. Технологии корпоративных сетей. Энциклопедия. — СПб.: Питер, 2000. — 704 с.
- [2] RFC 4306 Internet Key Exchange (IKEv2) Protocol.

## ИССЛЕДОВАНИЕ DNS-ЗАПРОСОВ С ЦЕЛЬЮ ПОИСКА ПОДОЗРИТЕЛЬНОЙ СЕТЕВОЙ АКТИВНОСТИ

Д.В. Демьяненко, С.В. Калинин, Е.В. Подмоков

*ННГУ им. Н.И. Лобачевского*

В наше время повсеместно используются информационные технологии и информационные системы, поэтому встает вопрос соблюдения политики безопасности. Существует множество уязвимостей не только в устройствах передачи информации, но и в протоколах, по которым реализуется взаимодействие систем с внешним миром, поэтому сильно возрастает риск нарушения безопасности. До сих пор остаются актуальными протоколы, которые были разработаны раньше, чем сетевые технологии настолько сильно вошли в нашу жизнь. В своём большинстве проблемы решались частично или полностью, разрабатывались средства для их нейтрализации. Не обошло это и протокол DNS, который не так давно получил 'обновление' – DNS SEC. С модернизацией протокола выросли и требования, например, устройства обязаны общаться только по TCP соединениями, что часто невыгодно, и сервер и клиент должны иметь поддержку DNS SEC. Кроме того возросла и сетевая нагрузка протокола, увеличилась опасность атаки DNS Amplification. Так же не решилась проблема с атакой посредством отравления хэша. Но даже при условии защищенности системы нельзя исключить вероятность наличия уязвимостей «нулевого дня». Именно по этим причинам возникла идея провести исследование DNS-запросов на подозрительную активность.

Для анализа DNS-трафика на предмет наличия вредоносных воздействий написана программа на языке Perl. Программа исполняется на сервере с ОС FreeBSD и записывает результаты анализа в базу данных PostgreSQL. В программе используется набор критериев, основанных на статистическом анализе дампов реального трафика. Параметрами критериев являются размер пакета, тип пакета и времени жизни пакета. Введен показатель подозрительности suspicion, по умолчанию равный нулю. При срабатывании каждого из критериев для пакета к показателю подозрительности прибавляется единица. При достижении показателем некоторого значения, адресант помещается в blacklist таблицу базы данных, которая используется для дальнейшего экспертного анализа. Функция whitelist, используется для записи в одноименную таблицу заведомо легитимных источников.

Исследование состояло из двух этапов. Первый этап использовался для отладки программы с использованием DNS информации локального сервера. При этом определялись значения критериев анализа. На втором этапе использовался дамп реального сетевого DNS сервера.

В процессе анализа обработано более 30000 записей в базе данных. При первой проверке не заполнялся whitelist, так подозрительными оказались 4749, то есть 12.3%. После анализа трафика, который обычно приходит на сервер и добавления в whitelist достоверных источников была проведена повторная проверка, показавшая, что подозрительный трафик был зафиксирован в 984 строках, что составило 2,6%.

<b>id</b>	<b>timestamp</b>	<b>dns_client</b>	<b>dns_server</b>	<b>rr_class</b>	<b>query</b>	<b>query_type</b>	<b>answer</b>	<b>ttl</b>	<b>count_s</b>	<b>suspicion</b>
360	1435661457.688314	85.143.5.39	85.143.0.30	IN	js.logetries.com.	CNAME	js-1746875212.eu-wA	1299	1	1
361	1435661457.688314	85.143.5.39	85.143.0.30	IN	js-1746875212.eu-wA	A	46.137.73.177	60	1	3
362	1435661457.688314	85.143.5.39	85.143.0.30	IN	js-1746875212.eu-wA	A	54.246.97.174	60	1	3
363	1435661457.688314	85.143.5.39	85.143.0.30	IN	js-1746875212.eu-wA	A	54.75.230.248	60	1	3
364	1435661460.500141	85.143.5.39	85.143.0.30	IN	api.skype.com.	CNAME	clientapi.skype.aka	37	1	1
365	1435661460.502238	85.143.5.39	85.143.0.30	IN	clientapi.skype.akadr	A	91.190.218.17	336	1	1

На рисунке приведен фрагмент базы данных. Строки 360-363 не прошли проверку значения TTL, длину запроса и количество цифр. При последующей проверке подтвердилась подозрительность, так как по результатам сканирования домена компанией VirusTotal на нём содержались вредоносные данные. На том же источнике были найдены и данные о 364-365, который не прошёл проверку по длине. Также изучена blacklist таблица, сформированная программой и весь объем данных, где критерий подозрительности был больше нуля. В результате экспертного анализа и данных из различных источники, таких как Kaspersky Labs и VirusTotal, реальная подозрительность была найдена в 745 строках, что составило 1,9% от общего объема данных.

В дальнейшем планируется доработка критериев для анализа трафика для уменьшения вероятности ошибки, а так же работа над алгоритмом программы с целью ускорения процедуры анализа.

## АНАЛИЗ БИЗНЕС-ПРОЦЕССОВ С ТОЧКИ ЗРЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.В. Корюкалов<sup>1)</sup>, Л.Ю. Ротков<sup>1)</sup>, И.Ю. Сорокин<sup>2)</sup>

<sup>1)</sup> ННГУ им. Н.И. Лобачевского

<sup>2)</sup> Союз Торговых Электронных Площадок

В задачах обеспечения информационной безопасности (ИБ) на уровне отдельной организации всегда присутствует актуальный вопрос оценки уровня защищенности. Оценка дает возможность определить текущее состояние и описать минимальный приемлемый (целевой) уровень защищенности, а также оценить затраты на достижение этого уровня. На сегодняшний день наиболее часто такой оценке подвергаются средства защиты информации, объекты информатизации и системы менеджмента ИБ.

Особенности данных объектов оценки приведены в [1]. Учитывая их, наряду с традиционными процедурами оценки представляется целесообразным рассмотреть в качестве объекта оценки бизнес-процесс. Предполагается, что такая оценка будет более информативной для руководителя организации, принимающего ключевое решение о выделении средств на повышение уровня защищенности.

Анализ исследований в данной области приведен в [1]. В ряде существующих работ предлагается учитывать особенности бизнес-процессов при решении задач ИБ. Вместе с тем, в проанализированных исследованиях не рассматривается возможность количественной оценки рисков ИБ на основе бизнес-процессов.

В рамках данной работы проанализированы бизнес-процессы проведения торгов в электронной форме по продаже имущества должников с использованием открытой и закрытой форм представления предложений о цене, описанные в [2-3].

При анализе бизнес-процессов преследовалась цель описать возможные риски информационной безопасности, ущерб от которых будет являться значимым для оператора электронной площадки (риски, связанные с неблагоприятными последствиями для других участников бизнес-процесса и не представляющие опасности для оператора, не рассматривались).

При определении рисков технические особенности реализации электронной площадки и способы реализации соответствующих угроз во внимание не принимались. Анализ проводился исключительно на основе влияния нарушения свойств безопасности информации на достижение целей оператора.

В результате анализа выделено три основных риска:

1. Нарушение доступности площадки для всех участников торгов.
2. Нарушение доступности площадки для отдельных участников торгов.
3. Нарушение конфиденциальности предложения о цене (при использовании закрытой формы представления предложений о цене)

Во всех трех случаях получена оценка возможного ущерба в денежном выражении экспертным методом.

Также сформулированы предложения по классификации угроз ИБ с точки зрения бизнес-процесса:

1. По характеру негативных последствий
  - 1.1. Остановка процесса
  - 1.2. Некорректное выполнение процесса (за счет искажения информации, на основе которой принимаются решения)
  - 1.3. Снижение эффективности процесса
  - 1.4. Нарушение требований законодательства
2. По моменту реализации угрозы
  - 2.1. До начала анализируемого процесса
  - 2.2. Во время анализируемого процесса
3. По времени проявления последствий от реализации
  - 3.1. Влияет на анализируемый процесс
  - 3.2. Проявляется позже

Полученные результаты показали, что в рамках данной предметной области с помощью анализа бизнес-процессов имеется реальная возможность количественной оценки ущерба. Однако, для определения величины целесообразных вложений в повышение уровня защищенности необходима количественная оценка рисков. Величина риска определяется совокупностью ущерба и вероятности реализации угрозы, а для оценки вероятности необходимо принимать во внимание особенности реализации информационной системы.

Дальнейшее исследование планируется продолжить в следующих направлениях:

1. Определение необходимых и достаточных сведений, подлежащих включению в модель бизнес-процесса, для его анализа с точки зрения ИБ.
2. Анализ различных бизнес-процессов и поиск областей, в которых возможен количественный анализ рисков ИБ.

- [1] Корюкалов А.В., Ротков Л.Ю. Бизнес-процесс как объект оценки уровня информационной безопасности / Образование, наука и технологии: современное состояние и перспективы развития: сборник научных трудов 31 октября 2015 г. / Под общ. ред. А.В. Туголукова – Москва : ИП Туголуков А.В., 2015 – С. 8.
- [2] Порядок проведения торгов в электронной форме по продаже имущества или предприятия должников в ходе процедур, применяемых в деле о банкротстве (утвержден Приказом Минэкономразвития России от 23.07.2015 № 495).
- [3] Федеральный закон от 26.10.2002 № 127-ФЗ «О несостоятельности (банкротстве)».

Секция «Информационные системы. Средства, технологии, безопасность»

Заседание секции проводилось 19 мая 2016 г.

Председатель секции – Л.Ю. Ротков, секретарь – А.А. Рябов.

Нижегородский государственный университет им. Н.И. Лобачевского.