3. Григорьев В. А. Сети и системы радиодоступа / В. А. Григорьев, О. И. Лагутенко, Ю. А. Распаев. – М.: Око-Трендз, 2005. – 384 с.

4. Волков Л. Н. Системы цифровой радиосвязи: базовые методы и характеристики: учебное пособие / Л. Н. Волков, М. С. Немировский, Ю. С. Шинаков. – М.: Эко-Трендз, 2005. – 392 с.

5. Теорія електричного зв'язку. Ч. 1: Основи теорії сигналів та розподілу інформації: підручник / О. В. Кувшинов, С. П. Лівенцев, О. П. Лежнюк [та ін.]. – К.: ВІТІ НТУУ „КПІ", 2008. – 331 с.

6. Кувшинов О. В. Аналіз способів підвищення ефективності систем рухомого радіозв'язку з кодовим розділенням сигналів / О. В. Кувшинов, С. П. Лівенцев // Збірник наукових праць ВІТІ НТУУ "КПІ". – 2004. – Вип. № 3. – С. 91-96.

7. Ільченко М. Ю. Телекомунікаційні системи широкосмугового радіодоступу / М. Ю. Ільченко, С. О. Кравчук. – К.: Наукова думка, 2009. – 312 с.

8. Wilton A. Deploying Wireless Networks / Wilton A., Charity T. – Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, Sao Paulo: Cambridge University Press, 2008. – 380 p.

9. Голдсмит А. Беспроводные коммуникации / А. Голдсмит. – М.: Техносфера, 2011. – 904 с.

10. IEEE Std 802.16f-2005: IEEE standard for local and metropolitan area networks. Part 16: air interface for fixed broadband wireless access systems. Amendment 1: management information base (Amendment to IEEE Std 802.16-2004). – New York: IEEE-SA Standards Board, 2005. – 257 p.

УДК 004.99:519.237

Е.В. Петров, магистр
С.А. Нестеренко, канд. техн. наук
Черниговский государственный технологический университет, г.Чернигов, Украина

ПОВЫШЕНИЕ СЕКРЕТНОСТИ СТЕГАНОГРАФИЧЕСКОЙ ПЕРЕДАЧИ ДАННЫХ В ИНТЕРНЕТ-ПОТОКЕ

Сформулировано основные причины, позволяющие по характеристикам интернет-потока, управляемого протоколом TCP, обнаружить факт передачи стегосообщения. Предложено модификация протокола передачи стегосообщения, способная нивелировать проявление упомянутых выше особенностей передачи, и, таким образом, повысить ее секретность.

Сформульовано основні причини, які дозволяють за характеристиками інтернет-потоку, керованого протоколом TCP, виявити факт передачі стегоповідомлення. Запропоновано модифікацію протоколу передачі стегоповідомлення, яка здатна нівелювати прояв згаданих вище особливостей передачі, і, таким чином, підвищити її секретність.

In the paper present the basic reasons which allow to detect the fact of stego message transmitting by analysis the statistical flow characteristics of Internet stream driven by TCP protocol. A modification of the transmission protocol which can reverse the expression of the above-mentioned singularities of transmission, and thus, increase the secrecy of the transfer is proposed.

Постановка проблемы. Предметом данной статьи является один из аспектов информационной безопасности, то есть такого состояния информационной системы, при котором обеспечивается сохранность, целостность и необходимая недоступность данных в ней [4].

Задача защиты информации от несанкционированного доступа является неизменно актуальной во многих областях человеческой деятельности: военном деле, государственном управлении, медицине, обеспечении конституционных прав граждан и т. п. Исторически выделились два основных направления решения этой задачи, существующие и по сегодняшний день: криптография и стеганография. Целью криптографии является скрытие содержимого наблюдаемых сообщений за счет их шифрования. В отличие от неё, при стеганографии скрывается не только содержание передаваемого секретного сообщения, но и сам факт его существования или передачи [3]. Назовем это требование «С-принципом».

Сегодня доминируют криптографические методы защиты информации, они весьма совершенны и их множество. Что касается стеганографии, то она развивалась значитель-

но медленнее. Значительный импульс ее развитию дала переживаемая в настоящий исторический период очередная технологическая революция, связанная с информатизацией всех сторон жизни общества. Уменьшается значимость многих традиционных способов и технологий коммуникации. К числу таковых можно отнести традиционную проводную телефонию, эфирное и кабельное телевизионное, радиовещание, а также обычную почту. Новые подходы в защите информации имеют в своей основе тот фундаментальный факт, что вся передаваемая и получаемая информация представляется в цифровом виде. Появилась возможность встраивать стеганографические сообщения в цифровые данные, которые изначально имели аналоговую природу – это речь, аудиозаписи, изображения, видео. Известны [1] также предложения по встраиванию информации в текстовые файлы и в исполняемые файлы программ. Нельзя не отметить также тот факт, что в настоящее время в ряде стран мира были введены законодательные ограничения на использование средств криптографии. С другой стороны, обострение борьбы за правовую охрану интеллектуальной собственности создает повышенный интерес к стеганографии, стимулирует исследования в области «водяных знаков» и т. п.

Учитывая быстрый рост коммуникаций через Интернет, которые все больше и больше начинают заменять собой все прочие, особый интерес представляют способы передачи стеганограмм в интернет-потоке данных. Учитывая потребность в соблюдении С-принципа, представляется перспективным применять для этого приемы, основанные на управлении количественными параметрами основного протокола интернет-коммуникаций, а именно – TCP (Transmission Control Protocol- протокола управления передачей).

Анализ исследований и публикаций. В работе А.Т. Алиева и А. Н. Щербакова [1] рассмотрен метод лингвистической стеганографии, основанный на синонимичной замене с учетом контекста. В предлагаемом там методе используется ограниченный словарь синонимов и специальная база контекстно-зависимого употребления слов, использование которой позволяет значительно снизить вероятность серьезного искажения структуры и смысла исходного текста.

В [2] рассматриваются основные принципы компьютерной стеганографии и области её применения, делается обзор известных стеганографических методов и приводятся сравнительные характеристики некоторых из них.

В статье W.Mazurczyk, M.Smolarczyk, и K.Szczypiorski [7] представлен метод стеганографии, названный авторами ретрансляционной стеганографией (RSTEG). Этот метод предназначен для широкого класса протоколов, в которых используется ретрансляция пакетов. Главное нововведение RSTEG в том, что для достижения целей передачи стегосообщения производится повторная передача части кадров. В статье также приводятся результаты моделирования, которые позволяют сравнить стеганографическую пропускную способность предложенного метода для различных механизмов ретрансляции, используемых в TCP.

Гендель и др. [8] описали метод стеганографии, который использует механизм повторной передачи после коллизии кадров. Если произошла коллизия кадров, то выдается сигнал, и отправителю возвращается кадр за определенный промежуток времени. Для отправки одного скрытого бита, инициализируются задержки различной длительности. Приемник извлекает стегоинформацию, анализируя порядок кадров прибытия после коллизии кадров.

Кратцер и др. [9] предложили метод стеганографии для стандартов связи группы IEEE 802.11, который передает скрытую информации с помощью ретрансляции кадров. Отправитель кодирует скрытые данные путем дублирования кадров, передаваемых приемнику. Приемник декодирует скрытые данные путем обнаружения дублирования.

В работах, описанных выше, есть ряд моментов, требующих дополнительного изучения и углубленной проработки для практического создания систем на основе описанных там алгоритмов. Например, в этих работах в качестве основы алгоритма часто используется ретрансмиссия – повторная передача кадров, вызванная либо тайм-аутом (кадр был послан, но за определенное время не дошел до адресата), либо адресатом. Ретрансмиссия является рутинной процедурой для протокола TCP, но при анализе трафика чрезмерная ретрансмиссия вызывает подозрение, и это приводит к обнаружению самого факта передачи, что нарушает постулированный выше С-принцип стеганографии. Поэтому необходимо учитывать количество передаваемой скрытой информации, которое в сообщении не может превышать некую предельную величину. Вместе с тем, ретрансмиссия может вызываться и естественными причинами, что усложняет алгоритм работы приемника сообщения в декодировании последнего. Чтобы вызвать ретранмиссию, необходимо программное вмешательство в работу сетевого контролера. Этот факт сразу указывает на специфичность программы, потому что необходимо либо применять специальный драйвер для сетевого контролера, либо создавать специальный программный модуль для контроля его работы. В закрытых операционных системах, подобных Microsoft Windows, этого достичь сложно. Очевидно также, что такая программа перестает быть кроссплатформенной и универсальной, что можно считать недостатком.

Наибольший интерес для нас представляет статья В.В. Орлова и А.П Алексеева [5], в которой рассматриваются принципы организации стеганографической системы (далее – «стегосистемы») в сети передачи данных на основе протоколов сетевого уровня. Предлагаемый метод скрытой передачи информации заключается в изменении длины сегмента таким образом, чтобы значение длины данных (число передаваемых символов), переносимых сегментом, содержало в себе информацию о секретном тексте. Коды символов секретного текста кодируются здесь значением длины данных, передаваемых очередным сегментом (L-кодирование). Часто для усиления защиты информации поверх стеганографии дополнительно используют еще и криптографию.

В качестве недостатка, описанного в [5] алгоритма, можно отметить то, что он ориентирован на кодирование только символов в кодировке ASCII, в силу чего им можно секретно передавать только текстовые сообщения. Кроме этого, чем больше по объему будут передаваемые скрытые сообщения, тем медленнее будет работать стеганографический алгоритм.

Цель статьи. Целью работы является анализ демаскирующих признаков стеганографической передачи информации в интернет-потоке и формирование приемов нивелирования их проявлений для повышения секретности канала передачи информации.

Реализация стегосистемы, использующей L-кодирование. Нами был реализован стеганографический алгоритм передачи секретных сообщений, в общих чертах подобный [5], но конкретизированный применением протокола TCP и расширенный введением дополнительной возможности передавать в потоке не только символы в кодировке ACSII, но также байты любого допустимого значения. Для данного алгоритма протокол TCP был выбран потому, что в отличие от UDP (User Datagram Protocol) он, во-первых, гарантирует целостность передаваемых данных и, во-вторых, в нем предусмотрено уведомление отправителя о результатах передачи.

Рассмотрим формат заголовка сегмента TCP и отметим важные поля для стегоалгоритма (табл. 1). Смещение данных определяет размер заголовка пакета TCP в 4-байтных (4-октетных) словах. Минимальный размер составляет 5 слов, а максимальный – 15, что составляет 20 и 60 байт соответственно. Смещение считается от начала заголовка TCP. Флаги – это поле содержит 6 битовых флагов, для данного алгоритма важен флаг со

смещением 2 PSH (Push function), который инструктирует отправителя вытолкнуть данные, накопившиеся в приемном буфере, в интернет-поток для передачи получателю.

Проиллюстрируем работу алгоритма на конкретном примере. Предположим, что секретное сообщение храниться в текстовом файле msg.txt, содержимое которого есть текст «Hello». Передаваемый файл, при помощи которого мы будем посылать скрытое сообщение, пусть называется File.txt, при этом содержимое файла может быть любым. Оба файла открываются для чтения, из msg.txt читаем первый байт, это символ «H», ASCII-код 72.

Таблиця 1

Заголовок сегмента TCP

Бит	**0–3**	**4–9**	**10–15**	**16–31**
0	Порт источника			Порт назначения
32	Номер последовательности			
64	Номер подтверждения			
96	Смещение данных	Зарезервировано	Флаги	Размер окна
128	Контрольная сумма			Указатель важности
160	Опции			
160/192	Данные			

Сервером передачи формируется TCP-сегмент, который должен перенести пользовательские (открытые, не содержащие секретных сведений) данные. Но длина сегмента передаваемых открытых данных делается равной значению ASCII-кода скрытно передаваемого байта. Поэтому в данном конкретном случае для передачи формируется блок открытых данных длиной именно 72 октета. Для этого побайтно считывается передаваемый файл File.txt во временный буфер. Как только объем буфера будет равен значению байта в секретном сообщении, информация в буфере отправляется принимающей стороне. Далее буфер очищается и описанные действия повторяются для следующего символа в секретном сообщении.

На принимающей стороне для извлечения скрытого символа требуется вычислить длину данных, переносимых TCP-сегментом. Для извлечения информации из общей длины IP-дейтаграммы (поле Total Length) вычитается длина IP-заголовка $112 - 5 \cdot 4 = 92$ байт. Из полученного значения общей длины TCP-сегмента вычитается значение смещения данных (поле Data Offset) $92 - 5 \cdot 4 = 72$ байт. Полученное значение длины открытого текста трактуется как значение байта принятого секретного файла, в данном случае – кода символа «H».

В соответствии с описанием RFC 793 [11], данные пользователя, подготовленные для передачи по сети, должны накапливаться в буфере. Когда буфер заполняется, происходит отправка подготовленного таким образом сегмента данных адресату, но при этом очевидно, что пользователь лишен возможности управлять длиной упомянутого сегмента. Однако спецификация протокола TCP [10] допускает возможность выталкивания сегмента в сеть путем управления флагом проталкивания PSH. Действительно, если в заголовке TCP-сегмента выставлен флаг PSH, то программа TCP должна немедленно отправить все имеющиеся в буфере данные. Аналогично, на удаленной стороне программа-обработчик TCP, встретив флаг проталкивания, должна передать принятые в буфер приема данные программам протоколов верхних уровней.

Даже поверхностный анализ данного алгоритма показывает, что он обеспечивает передачу одного L-закодированного байта стегосообщения путем передачи в среднем 100-200 байтов основного потока. Этот факт следует оценивать двояко. С одной стороны, это говорит о невысокой скорости передачи, но, с другой стороны, это положительно характеризует эту технологию как высоко скрытную. Поэтому при разработке критериев оценки эффективности этой технологии необходимо учитывать обе стороны этого вопроса.

Описанный алгоритм в практических испытаниях показал вполне устойчивую работу, но при этом проявился дополнительный нежелательный эффект, демаскирующий факт передачи стегосообщения, что является нарушением постулированного выше С-принципа.

Поясним суть обнаружившегося эффекта. Как было описано выше, во время работы программы, которая просто передает данные, размер TCP-сегментов чаще всего составляет 16384 байт, что обусловлено логикой функционирования TCP-стека [11]. В то же время, при передаче стегосообщений размер TCP-сегментов не может превысить максимальное для байта значение 255, а при передаче текстовой информации он еще меньше, порядка 100. В случае перехвата злоумышленником интернет-потока, направляемого получателю, будет заметно изменение в статистическом распределении размера TCP-сегментов. На рис. 1 и 2 показаны типичные распределения для двух случаев:

- когда стегосообщение передается (рис. 1);
- когда стегосообщение не передается (рис. 2).

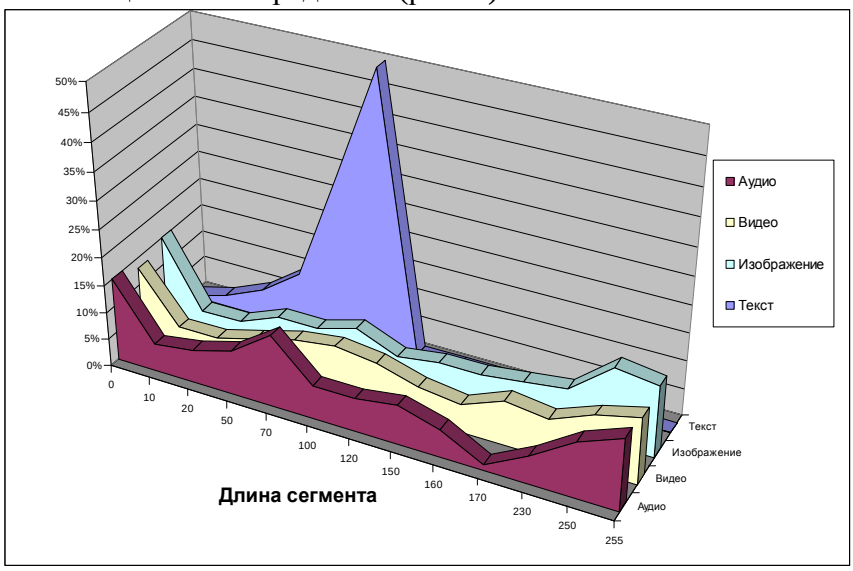

Рис. 1. Статистическое распределение длин TCP- сегментов при передаче стегосообщений различного типа

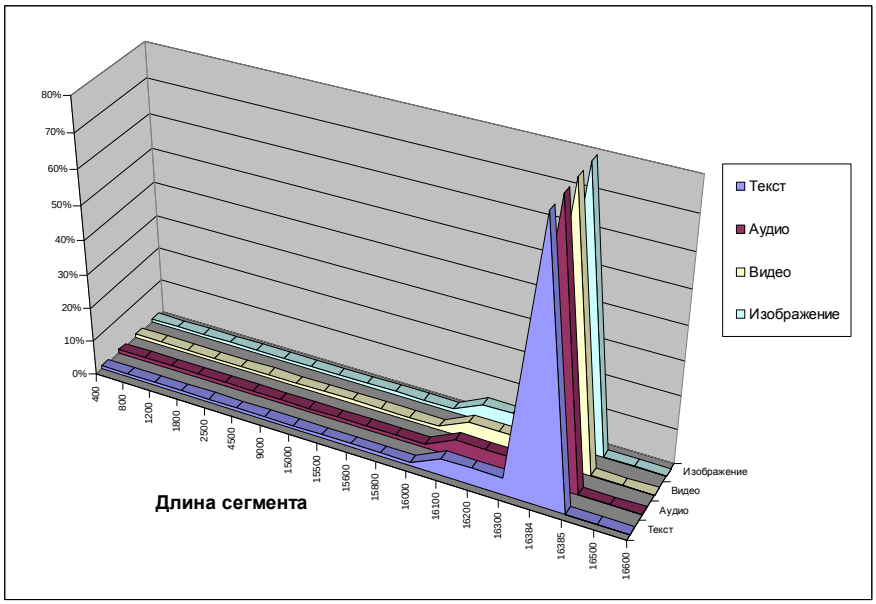

Рис. 2. Статистическое распределение длин TCP- сегментов при передаче обычных данных, без передачи стегосообщений

Это явление является демаскирующим и нарушает С-принцип стегостойкости системы. В связи с этим была предпринята попытка модернизировать алгоритм с целью изменить статистическое распределение длин TCP-сегментов при передаче стегосообщений в сторону максимального его приближения к таковому при отсутствии передачи.

Для этого было предпринято объединение блоков информации передаваемого файла в TCP-сегмент таким образом, чтобы его размер был как можно ближе к максимальному значению 16384. Поскольку в этом случае физический TCP-сегмент представляет собой объединение нескольких логических, возникла проблема выделения последних. Эта проблема была решена введением специальных разделителей логических субсегментов в общую последовательность байтов сегмента. Внешне статистическое распределение длин физических сегментов стало практически неотличимым от такового для случая отсутствия передачи, но потенциально демаскирующим теперь стало присутствие внутри физического сегмента разделителей. Учитывая тот факт, что отправитель и получатель могут динамически менять формат этих разделителей по заранее согласованным правилам, этой опасностью нарушения С-принципа можно пренебречь.

Результаты модификации алгоритма представлены на рис. 3:

а) статистическое распределение размера TCP-сегментов при передаче стегосообщения по модифицированному стегоалгоритму;

б) статистическое распределение размера TCP-сегментов при передаче основного интернет-потока без передачи стегосообщения.

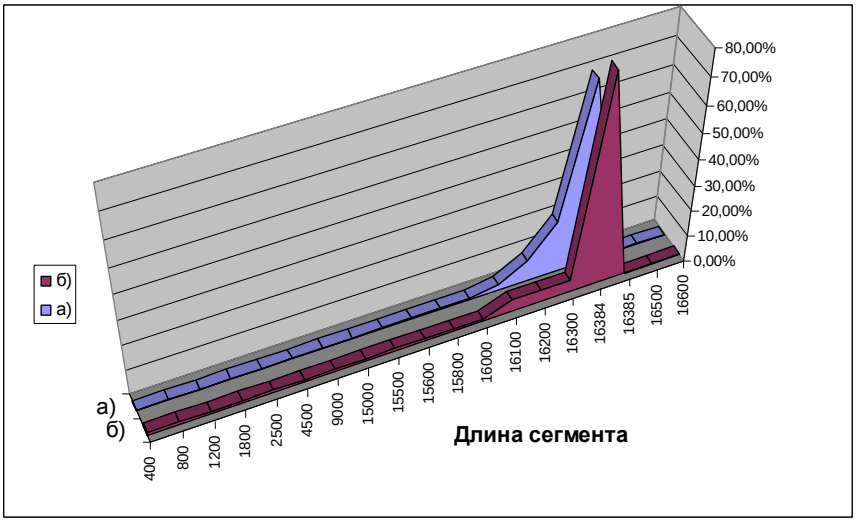

Рис. 3. Сравнение статистических распределений TCP-сегментов по их размеру при передаче стегосообщений по модифицированному алгоритму (а) и при обычной передаче потока без стегосообщений (б)

Выводы.

1. Управление числовыми параметрами процесса передачи данных в интернет-потоке под управлением протокола TCP следует признать перспективным методом стеганографии, имеющим практическую ценность.

2. Проявляющийся при этом демаскирующий эффект изменения статистического распределения длин TCP-сегментов может быть нивелирован применением объединения нескольких логических субсегментов в один физический.

3. Дальнейшее развитие работы возможно в сторону усовершенствования стеганографического алгоритма, алгоритма разбиения на фрагменты, использования криптографических методов, а также в направлении использования других характеристик протокола TCP для скрытой передачи данных.

Список использованных источников

1. Алиев А.Т. Стеганографический метод синонимичных преобразований открытого текста с учетом контекста / А.Т. Алиев, А. Н. Щербакова // Материалы III Международной научно-практической конференции / под общей ред. О. Н. Жданова, В. В. Золотарева; Сиб. гос. аэрокосмич. ун-т. – Красноярск, 2009. – 144 с.
2. Барсуков В. С. Компьютерная стеганография вчера, сегодня, завтра. Технологии информационной безопасности 21 века / В. С. Барсуков // Специальная техника. – 1998. – № 4-5.
3. Грибунин В. Г. Цифровая стеганография / В. Г. Грибунин [и др.]. – М.: СОЛОН-Пресс, 2002. – С. 2.
4. Информационная безопасность [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki.
5. Орлов В. В. Активная стеганография в сетях TCP/IP / В. В. Орлов, А. П. Алексеев // Инфокоммуникационные технологии. – 2009. – Т. 7. – № 2.
6. Стеганография [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki.
7. Mazurczyk W. Hiding Information in Retransmissions [Электронный ресурс] / Mazurczyk W., Smolarczyk M., Szczypiorski K. – Режим доступа: http://arxiv.org/abs/0905.0363.
8. Handel T., Sandford M. Hiding Data in the OSI Network Model, Proc. 1st International Workshop. Information Hiding, 1996. – P. 23-38.
9. Krätzer C., Dittmann J., Lang A., Kühne T. WLAN Steganography: a First Practical Review, Proc. 8th ACM Multimedia and Security Workshop., September 2006.
10. RFC 791 – Протокол IP (Internet Protocol) [Электронный ресурс]. – Режим доступа: http://rfc2.ru/791.rfc.
11. Transmission Control Protocol. Программная спецификация протокола. (RFC 793) [Электронный ресурс]. – Режим доступа: http://www.protocols.ru/files/RFC/rfc-793.pdf.

УДК 004.056.5:004.057.42

О.О. Фатіков, магістрант
В.В. Соломаха, ст. викладач
Чернігівський державний технологічний університет, м. Чернігів, Україна

КОМП'ЮТЕРНА СИСТЕМА ДЕТЕКТУВАННЯ НЕЯВНИХ МЕРЕЖЕВИХ АТАК

У статті розглянуто розробки архітектури комп'ютерної системи детектування й документування мережевих атак з використанням обманних методів.

Вступ. Одним з перспективних напрямків у побудові систем захисту інформації в наш час вважається застосування в системах захисту інформації обманної тактики [1; 2].

Обманна тактика захисту інформації дозволяє відвертати увагу порушників від основних цілей, заманюючи на неправильні інформаційні об'єкти, робити збір інформації щодо приймання, тактики й мотивації зловмисників, здійснювати їхню ідентифікацію й викриття.

Для виконання цих завдань можуть бути використані обманні системи, які називають також неправильними інформаційними системами, імітаторами інформаційних систем або системами-пастками. Основними функціями таких систем є залучення й утримання уваги зловмисників на неправильних інформаційних цілях, введення зловмисників в оману, виявлення й фіксація дій порушників, їх контроль, а також збір і агрегація даних про дії порушників з різних джерел.

Обманні системи являють собою програмно-апаратні засоби забезпечення інформаційної безпеки, що реалізують функції приховання й камуфляжу, що захищаються, інформаційних ресурсів, а також дезінформації порушників [1; 2; 3].

У цей час знаходять застосування два основні способи побудови обманних систем.

Системи, побудовані першим способом, називаються системами з низьким рівнем взаємодії. Ці системи емулюють програмно комп'ютери, операційні системи й сервіси.