Его достоинствами также являются простота реализации, неизменность размера файла-контейнера, возможность скрывать в относительно небольших файлах большие объемы информации. Кроме того, доказано, что данный метод позволяет получить наименьший уровень визуальных искажений [3].

Сущность этого метода отображена в самом его названии и заключается в замене наименее значащих бит контейнера — файла, в который будет встраиваться скрытая информация.

Известно, что человек воспринимает не всю информацию, заложенную в изображении, и если заменить у цветовых компонентов пикселя менее значащие биты на биты скрываемого сообщения, то выявить человек этого на глаз не сможет. Проводя последовательно подобную замену, начиная с заранее оговоренного пикселя, мы можем внедрить сообщение в файл-изображение. В качестве преимуществ этого метода сокрытия можно выделить его простоту реализации и большой объем данных, встраиваемый в передаваемый файл. Простой в реализации метод замены наименее значащего бита эффективен при решении задачи контроля целостности и защиты от фальсификации, при этом не требуется больших вычислительных ресурсов.

Таким образом, внедрение ЦВЗ методом замены наименее значащего бита решает проблему проверки целостности электронных документов в архиве, а восприимчивость этого метода к любым искажениям в этом применении является его главным достоинством.

СПИСОК ЛИТЕРАТУРЫ:

1. *Грибунин В. Г., Оков И. Н., Туринцев И. В.* Цифровая стеганография. М.: Солон-Пресс, 2002. С. 6–8.
2. *Кованович Г. Ф., Пузыренко А. Ю.* Компьютерная стеганография. Теория и практика. К.: МК-Пресс, 2006. С. 76–89.
3. *Вовк О. О., Астраханцев А. А., Дорожан А. В.* Исследование стойкости методов скрытия информации в неподвижных изображениях // Радиоэлектронные и компьютерные системы 2012, № 2 (54). С. 104-105.

К. В. Иванов

ПРОБЛЕМНО-ОРИЕНТИРОВАННАЯ МЕТОДИКА ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УЧЕТА И КОНТРОЛЯ ЯДЕРНЫХ МАТЕРИАЛОВ

Ввиду особенностей информации, обрабатываемой в автоматизированных системах учета и контроля ядерных материалов (АСУиК ЯМ), одним из ключевых требований, предъявляемых к системам данного класса, является требование обеспечения высокого уровня защиты информации от несанкционированного доступа. Наиболее сложные задачи, связанные с обеспечением информационной безопасности, возникают при создании систем, допускающих одновременную работу пользователей, обладающих различными правами на доступ к информации разных уровней конфиденциальности.

В работе рассмотрена проблемно-ориентированная методика построения систем защиты информации от несанкционированного доступа в АСУиК ЯМ, допускающих одновременную работу пользователей, обладающих различными правами на доступ к информации разных уровней конфиденциальности:

– не требующая сертификации средств защиты информации ОС и СУБД;

– предусматривающая модификацию программного обеспечения в интересах конкретного предприятия без модификации комплекса средств защиты информации.

Данная методика была применена для создания системы учета и контроля ядерных материалов ACCORD-2005, которая сертифицирована ФСТЭК по требованиям безопасности и допускает обработку информации, содержащей государственную тайну.

СПИСОК ЛИТЕРАТУРЫ:

1. Требования по защите от несанкционированного доступа к информации в автоматизированных системах учета и контроля ядерных материалов. Гостехкомиссия России, Министерство Российской Федерации по атомной энергии. М., 1997.
2. *Анищенко А. А., Иванов К. В.* Разграничение доступа в автоматизированных системах учета и контроля ядерных материалов // Вопросы атомной науки и техники. 2008. № 2. С. 66–70.
3. *Румянцев А. Н.* От учета и контроля к управлению // Новости ФИС. 2004. № 5. С. 39–48.
4. *Федосеев В. Н., Мизин П. П., Шанин О. И.* Подход к программному обеспечению для российских СУиК следующего поколения // Новости ФИС. 2003. № 3. С. 21–30.
5. *Щеглов А. Ю.* Защита компьютерной информации от несанкционированного доступа. СПб.: Наука и Техника, 2004. – 384 с.

С. Е. Кириллов, Н. П. Лаврентьев

ПОИСК УЯЗВИМОСТЕЙ СЕТЕВЫХ ПРИЛОЖЕНИЙ МЕТОДОМ ПСЕВДОСЛУЧАЙНОГО НАГРУЗОЧНОГО ТЕСТИРОВАНИЯ

Осуществление нормального обмена информацией посредством сети является критическим для существования современного общества, что делает актуальной задачу тестирования безопасности сетевых приложений. Большая часть угроз информационной безопасности сетевых приложений связана с наличием уязвимостей, вызванных ошибками при разработке и кодировании. Для поиска ошибок широко применяется методика псевдослучайного нагрузочного тестирования. При псевдослучайном нагрузочном тестировании на вход программы подаются специальным образом сформированные входные данные и отслеживается корректность выполнения программы на этих входных данных. Известны две разновидности такого тестирования [1, 2]: мутационное тестирование и генерационное тестирование. При мутационном тестировании в валидные входные данные внедряются искажения, такие как вставки, замены и удаления блоков информации. Генерационное тестирование подразумевает использование модели данных для генерации множества тестовых данных. В общем случае оба этих подхода имеют большое количество тестовых входных данных. Для сокращения пространства возможных входных данных при тестировании безопасности сетевых приложений необходимо знание достаточно точной модели форматов данных исследуемого приложения. Множество форматов сетевых сообщений задается в формализованном описании сетевого протокола. Для закрытых протоколов создание модели входных данных (определение структуры сообщений/сессий) требует обратной разработки, которая, если проводить анализ вручную, в ряде случаев может иметь высокую сложность.

В данной работе проведена доработка ранее разработанного алгоритма восстановления сессий, а также приведен алгоритм восстановления структуры сессий исследуемого сетевого протокола, идейно продолжающий предложенный в [3] подход. На вход алгоритма поступает собранная трасса валидных взаимодействий в рамках исследуемого протокола. Первоначально из трассы выделяются отдельные сообщения, в которых ищутся текстовые, и выполняется первичная