

Список литературы

1. Концепция информационной безопасности Республики Беларусь: утв. Постановлением Совета Безопасности Республики Беларусь 18.03.2019 № 1.

ПРОБЛЕМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СЕТЕЙ

Р.В. Кислинский

В силу технического прогресса все больше информации на предприятиях и в государственных учреждениях обрабатывается сегодня с использованием средств вычислительной техники. Как следствие, возникает проблема защиты обрабатываемой на средствах вычислительной техники и передаваемой информации.

При построении необходимого уровня защиты информации возникает ряд проблем, которые требуют применения методов анализа и специфических организационных методов и процедур по защите информации.

Основные проблемы защиты информации можно разделить на три группы:

- нарушение конфиденциальности информации;
- нарушение целостности информации;
- нарушение доступности информации.

При построении защиты используются программные решения в области информационной безопасности, но при использовании программных продуктов для построения системы защиты сети возникает ряд проблем:

- расширенная зона контроля;
- неизвестный периметр;
- сложность в управлении и контроле доступа к системе;
- множество точек атаки;
- использование различных программно-аппаратных комплексов защиты информации;
- скрытые каналы утечки информации.

Список литературы

1. Бормотов В.Е. Проблемы защиты информации в компьютерной сети // Молодой ученый. 2016. № 11. С. 148-150. URL <https://moluch.ru/archive/115/31145/> (дата обращения: 27.09.2018).

2. Программно-аппаратная защита информации / под ред. С.К. Варлатая, М.В. Шаханова. Владивосток: ДВГТУ, 2007. 243 с.

3. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах. М.: ИНФРА-М, 2010. 592 с.

МЕТОДЫ ВНЕДРЕНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ В ПОТОКОВОЕ ВИДЕО

Т.Ю. Кишкурно, М.М. Данильчик

Противодействие незаконному копированию цифровой информации всегда являлось актуальной задачей, а сегодня, в условиях полной информатизации общества, защита становится все более и более важной. Внедрение цифровых водяных знаков (ЦВЗ) в видеоданные применяется для обеспечения защиты цифровых данных и помогает предотвратить копирование, тиражирование и прочие возможные варианты коммерческого использования информации третьими лицами [1].

В работе проанализированы методы внедрения ЦВЗ в потоковое видео такие как: дискретное косинусное преобразование (ДКП, DCT), алгебраическое преобразование, дискретные вейвлет-преобразования (ДВП), алгоритм синхронизации. Разработана шкала для оценки эффективности методов внедрения цифровых водяных знаков. Основными

критериями оценки эффективности являются: вычислительная мощность и сложность алгоритма, зависимость положения ЦВЗ относительно других кадров видеоряда.

Алгоритм ДКП, основанный на дискретно-косинусном преобразовании сигнала использует относительно емкие для процессора формулы нахождения косинусов соответствующих величин. Алгоритм, основанный на вейвлет-преобразовании сигнала (ДВП, преобразование Хаара), возможно реализовать в виде самых быстрых для вычисления математических операций процессором, что значительно экономит время по сравнению с ДКП. С помощью алгоритма синхронизации внедрение и извлечение ЦВЗ проходит с большим коэффициентом корреляции (близким к единице), вследствие чего вычислительная нагрузка становится меньше.

Список литературы

1. Григорьян А.К., Аветисова Н.Г. Методы внедрения цифровых водяных знаков в потоковое видео. Обзор // Информационно-управляющие системы. 2010. № 2. С. 38–45.

ИДЕНТИФИКАЦИЯ СООБЩЕНИЙ ОЦЕНКАМИ ЧИСЛА ВЕКТОРОВ ПЕРЕХОДОВ

И.П. Кобяк

В представляемой работе рассматривается метод синтеза оценок вероятности регистрации двоичных (01)-переходов при решении задач идентификации сообщений [1]. Получено соотношение для вероятности пропуска ошибки, соответствующее указанному алгоритму при наблюдении компьютерами априори неопределенной асимптотической выборки. Определена мода распределения и выполнен сравнительный анализ вероятностей пропуска ошибки, характеризующих предлагаемый метод и известные алгоритмы свертки в точке моды. По результатам работы сделаны следующие выводы: 1) двоичные переходы могут отождествляться с событиями АКФ некоторого заданного вида; 2) графики функций вероятностей пропуска ошибки, соответствующие наблюдению переходов и формированию линейных сигнатур не имеют в асимптотике точек пересечения; 3) из вывода два следует, что метод наблюдения переходов в вероятностных процессах является более точным методом идентификации, чем сигнатурный анализ; 4) аналогичный вывод в пользу АКФ специального вида для двух заданных событий аналитически подтвержден и при сравнении исследуемого метода с алгоритмом наблюдения бернуллиевских 0 или 1 элементарных состояний. Следует ожидать, что улучшение показателей, характеризующих методы идентификации двоичной выборки в системах идентификации сообщений, может быть достигнуто в рамках синтеза других более сложных событий на базе ряда заданных состояний исследуемого процесса. При этом должна учитываться динамика формирования отсчетов для различных сдвигов, а также возможно иные, формально не определенные на сегодняшний день свойства объектов с технической, информационной или другой дискретной природой.

Список литературы

1. Кобяк И.П. Сравнительный анализ вероятностей пропуска ошибки при синтезе сигнатур и оценок числа векторов переходов // АВТ. 2004. № 5. С. 50–57.

ФИЗИКА АТОМА В РАСЧЕТАХ КРИПТОГРАФИЧЕСКИХ КАНАЛОВ СВЯЗИ

И.П. Кобяк

На основе традиционной концепции формирования спектра атома водорода получено уравнение для энергии, излучаемой электроном при переходе с энергочувствительного уровня с номером n на энергочувствительный уровень боровского радиуса. Получены соотношения, характеризующие параметры центроаффинного пространства ядра [1], а также равенство для эквивалента массы излучаемой энергии. Решение энергетического уравнения позволило рассчитать значения всех радиусов энергочувствительной «классического» атома и соответственно скорости электрона на данных