

Математическое обеспечение системы обработки видеоданных, разделяемых для передачи по двум каналам связи с целью их защиты

Рассмотрены вопросы разработки математического обеспечения системы обработки видеоданных, выполняющей разделение кадров потока видеоданных для организации их защищенной передачи от кибервмешательства по двум параллельным каналам связи. Каждый кадр, называемый секретом, делится на две неравные доли, передаваемые по каналам связи, имеющим различные пропускные способности. Решается задача оптимизации пропускных способностей двух каналов связи по критерию минимизации взвешенной суммы временных и стоимостных затрат на защищенную передачу видеоданных. Получена аналитическая зависимость времени задержки на передачу видеоданных от пропускных способностей каналов связи, пригодность которой для практического использования подтверждена экспериментально. Разработанное математическое обеспечение системы обработки видеоданных позволяет определить оптимальные пропускные способности каналов связи при выполнении демультиплексирования по ним долей кадров передаваемого потока видеоданных, а также позволяет оценить издержки на содержание такой системы.

Ключевые слова: защита информации, разделение секрета, видеоданные, пропускная способность, демультиплексирование, мультиплексирование, кибервмешательство.

Сагайдак Дмитрий Анатольевич – аспирант Омского государственного технического университета (ОмГТУ).

Список литературы

1. Shamir A. How to share a secret / A. Shamir // Communications of the ACM 22. 1979. P. 612-613.
2. Sagaydak D. A., Faizullin R.T. Model secret sharing schemes in systems transmit video // Computer Optics. 2013. Vol. 37. N 1. P. 105-112.
3. Файзуллин Р.Т., Сагайдак Д.А. Приложение алгоритма префиксного кодирования массива данных в схеме разделения секрета потока видеоданных // Тр. Томского государственного университета систем управления и радиоэлектроники. 2012. № 1-2(25). С. 136-140.
4. Михеев В.В., Сагайдак Д.А., Свенч А.А., Файзуллин Р.Р. Алгоритмы обработки информации при передаче и хранении данных, основанные на процедуре разделения секрета // Вестник Сибирской государственной автомобильно-дорожной академии. 2012. № 5(27). С. 82-87.
5. Клейнрок Л. Вычислительные системы с очередями. - М.: Мир, 1979. – 600 с.
6. Алиев Т.И. Основы моделирования дискретных систем. – СПб: СПбГУ ИТМО, 2009. – 363 с.
7. Уоллэнд Дж. Введение в теорию сетей массового обслуживания - М.: Мир, 1993. - 336 с.
8. Программа, реализующая алгоритм префиксного кодирования видеoinформации, основанного на примитивизации дельта-кода Элиаса в схеме разделения секрета с принципиально малой частью секрета: свидетельство о государственной регистрации программы для ЭВМ. № 2013661611 РФ / Д. А. Сагайдак; заявл. 25.10.13; publ. 20.01.14, 1 с.

Sagaidak D.A. Video data processing software aimed at two-channel data separation for security purposes

The paper discusses the development of software for a video data processing system, which separates the frames

of video data stream in two parallel communication channels for protecting them against cyber interventions. Each frame called a secret is split into two unequal parts communicated through separate channels with different capacities. The capacities of two channels are optimized by minimizing the weighted sum of time and cost expenses for secure video data transfer. A mathematical relationship between data transfer delay time and the capacities of communication channels is obtained; the experiments prove its practical applicability. The software developed enables the evaluation of optimal capacities of data communication channels for the demultiplexing of frame shares of the video data stream transferred as well as the estimation of overall system maintenance costs.

Keywords: *information protection, secret splitting, video data, channel capacity, demultiplexing, multiplexing, cyber intervention.*