формирования раундовых ключей по ступеням конвейера с использованием массива регистров перемещаются входные ключи, а не сами раундовые ключи. Такой подход позволяет получить более экономичную реализацию генератора ключей и конвейера алгоритма шифрования данных в целом.

Характеристики реализации процессора зашифрования с 32 конвейерами алгоритма DES после процесса MAP с использованием пакета ISE 14.7 для кристалла FPGA семейства Virtex7 XC7VX485T-1: 60027 триггеров секций, 48794 просмотровых таблиц (LUT), рабочая тактовая частота – 283 МГц.

Список литературы

1. McLoone M., McCanny J.V. High-performance FPGA implementation of DES using a novel method for implementing the key schedule // IEE Proc.-Circuits Devices Syst. 2003. Vol. 150, No. 5 URL: https://www.researchgate.net/ publication/3349437_High-performance_FPGA_ implementation_of_DES_using_a_novel_method_for_implementing_the_key_schedule (дата обращения: 03.05.2019).

НЕКОТОРЫЕ АСПЕКТЫ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ НА КАФЕДРЕ ИНЖЕНЕРНОЙ ПСИХОЛОГИИ И ЭРГОНОМИКИ БГУИР

П.И. Кирвель, Д.А. Мельниченко

В соответствии с Концепцией информационной безопасности Республики Беларусь цифровая трансформация экономики является важнейшей составляющей формирования информационного общества и одним из главных направлений устойчивого развития Республики Беларусь, в результате которого в ближайшие десятилетия все отрасли, рынки, сферы жизнедеятельности государства должны быть переориентированы на новые цифровые экономические модели. Для решения этой задачи первостепенное значение имеет подготовка высококвалифицированных информационно- и практико- ориентированных специалистов в области защиты информации.

На кафедре инженерной психологии и эргономики проводится планомерная работа по подготовке специалистов в данной области: начиная с первой ступени высшего образования по специальностям «Инженерно-психологическое обеспечение информационных технологий» и «Информационные системы и технологии (в обеспечении промышленной безопасности)», с последующим углубленным обучением на второй ступени высшего образования по специальности «Управление безопасностью производственных процессов».

На кафедре разработан новый электронный учебно-методический комплекс по дисциплине «Информационные системы обеспечения безопасности» для подготовки магистров. Целью изучения данной дисциплины является формирование у магистрантов системы знаний об особенностях создания, функционирования и управления информационными системами в современных условиях развития общества, а так же освоение практико-ориентированных учебных материалов по применению инновационных стратегий, технологий и методов обеспечения безопасности в условиях производства и эксплуатации современных технических и программных средств, реализующих информационные технологии. После изучения дисциплины мы получим специалиста, обладающего комплексными предметными знаниями в области создания и управления информационными системами, адаптации и использования этих систем и технологий в профессиональной деятельности, а также имеющего навыки инновационной деятельности в области защиты информационных потоков в современных условиях развития общества.

Это, безусловно, будет способствовать формированию в Республике Беларусь прогрессивного информационного общества, обеспечивающего доступность информации, распространение и использование знаний для поступательного и передового развития.

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