

не верифицирует версии файлов проектов после многократных сборок и выпусков программных продуктов.

Целью настоящей работы явилась разработка программного продукта, интегрируемого в TFS, обеспечивающего верификацию изменений версий файлов.

При разработке программного продукта использовалась возможность от компании Microsoft [1] расширения интегрированной среды разработки Visual Studio с внедрением в систему контроля версий TFS с целью расширения ее функционала. Для создания необходимых графических окон представления программного продукта, использовалась технология Windows Presentation Foundation (WPF). Встраивание в систему контроля версий TFS осуществлялась один из подходов объектно-ориентированного программирования Application Programming Interface.

Таким образом разработан программный продукт как расширение (plugin) для интегрированной среды разработки (Integrated Development Environment) Visual Studio 2017, который путем интегрирования с системой контроля версий Team Foundation Server позволяет верифицировать изменения файлов при выпуске новой сборки программного продукта.

Литература

1. Arora T Microsoft Team Foundation Server Cookbook. UK: Birmingham B3 2PB, 2016. 309 p.

ПРОБЛЕМЫ КОДИРОВАНИЯ И ПЕРЕДАЧИ ВИДЕОИНФОРМАЦИИ В БЕСПИЛОТНЫХ АВИАЦИОННЫХ КОМПЛЕКСАХ

Г. Марун, Б.А. Голищев, В.В. Позняк, Г.А. Розум

В беспилотных летательных аппаратах используется одна или несколько видеокамер для передачи видеоизображений оператору. Высокая скорость формирования видеоинформации требует высоких коэффициентов сжатия при приемлемом качестве восстановления изображений. Известные кодеки, основанные на блочной, пиксельной и кадровой компенсации движения, обеспечивают сжатие в сотни – тысячи раз. Формируемый в результате сжатия видеопоток имеет сложную структуру с большим числом блоков, разноразмерных, и высокой зависимостью значений, принадлежащих различным блокам. Это требует использования помехоустойчивого кодирования, вносящего дополнительную избыточность в видеопоток, достигающую 30 %. В результате скорость передачи видеоданных возрастает, снижая положительный эффект от сжатия. Высокая скорость формирования видеоданных требует использования для их передачи высоких частот. При этом необходимо обеспечение прямой видимости между передатчиком и приемником данных, а также компенсация доплеровского эффекта. Кроме того, возникают ограничения со стороны элементной базы – требуется высокая скорость обработки сигналов в модуляторе, кодере, декодере и демодуляторе, что приводит к высокому энергопотреблению. Перечисленные особенности свидетельствуют об актуальности задачи разработки новых эффективных методов сжатия видеоинформации, позволяющих существенно снизить скорость видеопотока, использовать для передачи относительно низкие частоты и низкоскоростную элементную базу. Исследования в данном направлении связаны, как с повышением эффективности кодирования результатов прогнозирования, так и с учетом новых видов избыточности видеоинформации, специфичных для определенных условий использования беспилотных авиационных комплексов. Последний подход позволяет достичь более высоких коэффициентов сжатия, но связан с существенной вычислительной сложностью, ограничивающей возможности бортовой обработки видеоинформации.

ПРИМЕНЕНИЕ НЕЛИНЕЙНЫХ ПОМЕХОУСТОЙЧИВЫХ КОДОВ В КАНАЛЕ С ПОДСЛУШИВАНИЕМ

А.И. Митюхин

Одно из применений нелинейных ортогональных конструкций $[N, M, d]$ -кодов длиной N и кодовым расстоянием d заключается в обеспечении определенного уровня защиты информации. Свойство нелинейности кода позволяет иметь значительно больший ансамбль

M кодовых слов X над полем Галуа в сравнении с линейными кодами, что важно для защиты информации. Рассматривается подход защиты кодированной информации в предположении, что преднамеренно генерируемые ошибки E в принятом сигнале и шумы n в канале с подслушиванием должны существенно увеличить значение вероятности ошибки декодирования кодового слова в условиях ограничения времени на анализ и обработку перехватываемого сигнала. В этом случае на входе декодера канала с подслушиванием формируется вектор наблюдения Y в виде трехкомпонентного аддитивного процесса: векторов слов кода X , векторов ошибок E и векторов шума n канала. Так как значения вероятностей $P(x)$ входа и $P(y)$ выхода основного канала априори известны и практически равны, то в соответствии с теоремой Байеса, зная переходные вероятности $P(Y|X)$ канала, легко можно найти вероятность $P(X|Y)$ правильного декодирования информации по основному каналу. Наилучшая процедура декодирования вектора наблюдения Y по каналу подслушителя состоит в нахождении такого значения номера кодового слова, при котором значение вероятности $P(Y|X)$ достигает максимума [1]. Поскольку в канале подслушителя функция $\max P(Y|X)$ зависит от большого числа M , от структуры векторов внедряемых ошибок E и векторов шума n , байесовская процедура нахождения вектора X ближайшего по расстоянию d к принятому вектору Y становится затратной с точки зрения необходимости значительных вычислительных, временных и технических ресурсов для успешного перехвата кодированной информации.

Литература

1. Митюхин А.И., Якубенко П.Н. Корреляционные спектры и кодовые расстояния мажоритарных последовательностей // Докл. БГУИР. 2015. № 4 (90). С. 5–9.

ИСПОЛЬЗОВАНИЕ МЕЖСЕТЕВОГО ЭКРАНА НОВОГО ПОКОЛЕНИЯ В КОРПОРАТИВНЫХ СЕТЯХ

А.Д. Михейчик, О.А. Хацкевич

На сегодняшний день практически все организации осуществляют информационную безопасность своей корпоративной сети, используя различные средства. К таким средствам можно отнести: антивирусные ПО, межсетевые экраны, DLP-системы, системы обнаружения и предотвращения вторжений. Проблема заключается в том, что если использовать комплексное решение по обеспечению информационной безопасности сети, то могут возникнуть случаи, когда одно средство по безопасности будем считать другое средство угрозой для сети. Данная проблема может возникнуть, если в качестве комплексного решения использовались средства по информационной безопасности различных производителей. Для решения проблемы предлагается использовать набирающие популярность в последнее время межсетевые экраны нового поколения (МЭНП).

Межсетевые экраны нового поколения (англ. Next-Generation Firewall) – это совокупность средств, в которые входят: межсетевой экран, система обнаружения и предотвращения вторжений, DPI-технология, DLP-система. Некоторые МЭНП, например Fortigate 3810A, могут поддерживать антивирусное ПО, а также обнаружения DoS-атак. Отличие от обычного меж сетевого экрана заключается в том, что МЭНП включает в себя больше уровней модели OSI, улучшая фильтрацию сетевого трафика, зависящую от содержимого пакета.

ОПЫТ ПРИМЕНЕНИЯ МЕТОДИКИ ОПРЕДЕЛЕНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Е.В. Моженкова, А.И. Парамонов

Корпоративная информационная система (КИС) должна обеспечивать не только ведение учета и формирование отчетов по национальным и международным стандартам, а также предупреждать попытки несанкционированного доступа к информации. Для определения угроз безопасности персональных данных (ПДн) при их обработке в информационных системах (ИС) в Российской Федерации разработана «Методика