Заключение

В данной работе были исследованы принципы обеспечения стойкости ЦВЗ к геометрическим искажениям. Результаты проведённого исследования показывают, что применение аппарата характеристических точек позволяет строить системы ЦВЗ, стойкие к геометрическим искажениям.

Благодарности

Работа выполнена при частичной финансовой поддержке грантов РФФИ (проекты 12-01-00822, 13-01-97007, 12-07-31056, 13-01-12080, 12-07-00021), гранта Президента РФ МК-3863.2013.9, министерства образования и науки Российской Федерации (в соответствии с постановлением Правительства России от 09.04.2010 № 218), программы фундаментальных исследований Президиума РАН «Фундаментальные проблемы информатики и информационных технологий», проект 2.12.

Литература

1. A survey of RST invariant image watermarking algorithms / D. Zheng, Y. Liu, J. Zhao, A.E. Saddik // *ACM Computing Surveys (CSUR)*. – 2007. – Vol. 39, №2. – C.3.

2. Bas, P. Geometrically invariant watermarking using feature points / P. Bas, J-M. Chassery, B. Macq // *Image Processing, IEEE Transactions on*. – 2002. – Vol. 11, №9. – P. 1014-1028.

3. Harris, C. A combined corner and edge detector / C. Harris, M. Stephens // In *Alvey vision conference*. – 1988. – Vol. 15. – P. 50.

4. Achard-Rouquet, C. Un détecteur de points caractéristiques sur des images multispectrales, extension vers un détecteur sub-pixellique / C. Achard-Rouquet, E. Bigorgne, J. Devars // GRETSI. – 1999. – P. 627-630.

5. Lowe, D.G. Distinctive image features from scale-invariant keypoints / D.G. Lowe // *International journal of computer vision*. – 2004. – Vol. 60, №2 – P. 91-110.

6. Mayer, G. Waterloo Grey Set Image Repository // University of Waterloo Fractal coding and analysis group – 2009 [Электронный ресурс]. URL: http://links.uwaterloo.ca/Repository.html (дата обращения: 10.04.2013).

А.А. Волков, Ю.Ю. Палунина, Н.Ф.Бахарева

АЛГОРИТМ АВТОМАТИЗИРОВАННОГО ПОСТРОЕНИЯ КОМЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

(Поволжский государственный университет телекоммуникаций и информатики)

В сфере информационной безопасности одним из ключевых аспектов построения системы защиты информации является её соответствие требованиям существующего законодательства: Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных», Приказ ФСТЭК России от 18.02.2013 № 21 «Об

утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Приказ ФСТЭК России от 11 февраля 2013 года N 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (вступает в силу с 1 сентября 2013 года) и др.

Данные требования зачастую изложены довольно абстрактно. В то время как для обеспечения их выполнения необходимо использовать конкретные средства защиты информации. Ими могут быть: программное обеспечение, программно-аппаратные комплексы, инженерные устройства, а так же различные организационные методы. Разнообразие существующих средств велико. Каждое из них закрывает ряд требований законодательства. Конкретные продукты, реализованные тем или иным производителем, отличаются друг от друга не только функционалом, но и списком закрываемых требований законодательства.

При построении комплексной системы защиты неизбежны ситуации, когда отдельно взятые средства пересекаются друг с другом и дублируют некоторые функции.

Проблема заключается в том, что алгоритм построения системы защиты информации, по сути, отсутствует. При построении системы разработчик основывается на известных ему средствах защиты информации, субъективном мнении и ряде сторонних факторов, зачастую не имеющих под собой объективных оснований, например, наличие партнёрских отношений с одним производителем и отсутствием таковых отношений с другим. Всё это может негативно сказаться на качестве разработанного решения, его стоимости и эффективности.

Для постановки задачи по разработке такого алгоритма, стоит прояснить, как происходит процесс построения системы защиты на практике. Данный процесс начинается с того, что проводится анализ следующих ключевых аспектов.

1. Исходные данные о самой информационной системе, которую требуется защитить: её размер, структура, состав и тип обрабатываемых данных, уже применяемые средства защиты информации и другие факторы.

2. Требования законодательства для данного типа информационной системы и обрабатываемых в ней данных.

3. Перечень средств, из которых возможно построить комплексную систему защиты.

4. Ряд внешних факторов: принятые в отрасли стандарты и привычные схемы защиты, знания сотрудниками конкретных платформ и средств защиты информации, особенности финансирования организации, особенности средств защиты: совместимость конкретных средств между собой, стоимость совокупного владения, сложность сопровождения и многое другое.

Огромное разнообразие факторов, влияющих на выбор средств, приводит к тому, что множество вариантов реализации системы защиты чрезвычайно велико. Построенные варианты реализации можно оценить по различным критериям.

1. Полнота перекрытия требований законодательства.
2. Бюджет внедрения системы защиты.
3. Стоимость и сложность дальнейшего сопровождения.
4. Единообразие применённых при построении средств и другие.

Существующая ситуация требует разработки автоматизированного алгоритма выбора средств при построении системы защиты. Для решения поставленной задачи и возможности применения математического аппарата, необходимо описать все входные данные и влияющие факторы. Для этого требуется решить следующие подзадачи :

1. Формализация критериев и оценочной шкалы для каждого средства защиты информации. Необходимо определить, какие свойства являются важными для оценки средства, а какие можно не учитывать.

2. Создание пополняемой базы данных по средствам защиты информации с фиксацией значимых свойств, определённых на первом шаге.

3. Формализация требований законодательства в области информационной безопасности и создание базы данных таких требований.

4. Выделение значимых внешних факторов, их описание и структуризация.

5. Выделение значимых свойств информационной системы, которые влияют на построение системы защиты.

Только после решения этих подзадач станет возможным разработка алгоритма построения системы защиты информации.

Алгоритм должен работать в несколько проходов и обеспечивать обратную связь на каждой итерации.

1. Выделить ключевые элементы системы защиты информации, покрывающие значительную часть требований и удовлетворяющие внешним факторам.

2. Учитывая выбранную основу, выполнить итерации выбора из базы данных по средствам защиты информации, дополняющие систему средства. Алгоритм должен быть направлен на снижение количества применяемых средств и максимальное соответствие всем требованиям и внешним факторам.

3. После того, как вся система будет спроектирована, необходимо провести её анализ с целью оценки по критериям, перечисленным ранее. В результате оценки системы, возможно внесение корректировок в изначальные условия построения системы защиты и перезапуск алгоритма.

Таким образом, можно заключить, что разработка алгоритма автоматизированного построения системы защиты информации является нетривиальной задачей. Поэтому в первую очередь требуется решить выделенные подзадачи, которые позволят заложить основу для разработки такого алгоритма.