УДК 004.932.2

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 2, pp. 163-168

НОВАЯ КЛАССИФИКАЦИЯ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ

Е.В. Нариманова, Е.А. Трифонова

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: semejka@ua.fm

Предложена новая классификация методов защиты информации с учетом методов проверки целостности цифровых сигналов, которые на сегодняшний день вызывают наибольший интерес, однако не имеют своего места в рамках методов и средств защиты информации.

Ключевые слова: классификация, методы защиты информации, методы проверки целостности, методы активной защиты информации, методы пассивной защиты информации

Введение

Процесс внедрения новых информационных технологий во все сферы жизни общества немыслим без решения вопросов информационной безопасности, которая структурируется в совершенно разных, но связанных между собой аспектах [1, 2] (рис. 1).

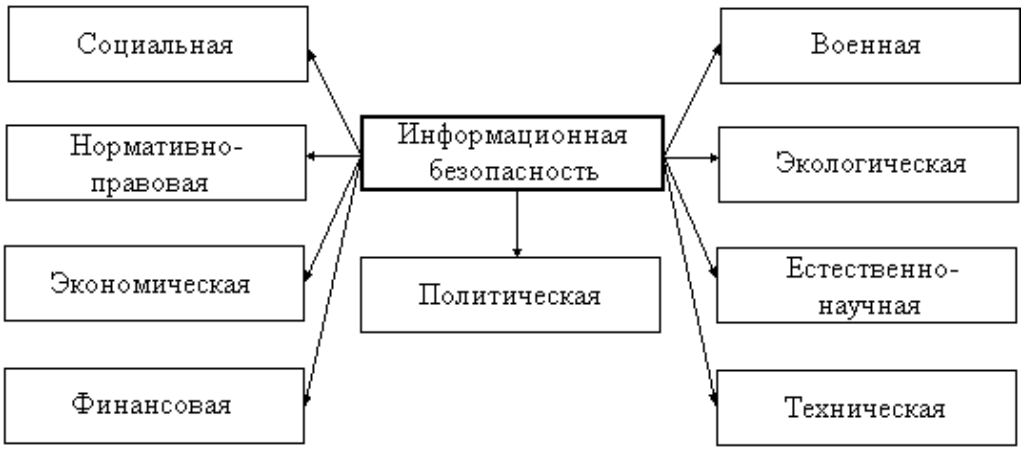

Рис. 1. Аспекты проблемы информационной безопасности

Широкомасштабное использование вычислительной техники и телекоммуникационных систем, переход к безбумажной технологии, увеличение объемов обрабатываемой информации и расширение круга пользователей приводят к качественно новым возможностям несанкционированного доступа к ресурсам и данным информационных систем, к их высокой уязвимости. В современных условиях возникает необходимость защиты не только государственной и военной, но и промышленной, коммерческой и финансовой тайн. Защита информации в целом, в том числе защита информации в автоматизированных системах, становится все более

актуальной и сложной проблемой, для решения которой необходимо построение общего системного комплексного подхода к защите информации.

Современная концепция комплексной защиты согласуется с идеями, высказанными еще в 1986 г. в [3], где впервые в отечественной печати затрагиваются вопросы перспектив развития теории защиты, принципиальные положения которой сформулированы чуть позже в [4], где комплексность защиты информации строго обоснованно ставится на первое место.

В [1, 2] представлен систематизированный обзор современного состояния и путей развития методов и средств защиты информации. Используемый для этого единый системно-концептуальный подход, в рамках которого проводится выделение в предметной области защиты информации трех иерархий: структурной, причинно-следственной и функциональной, рассматривающий и анализирующий все значительные факторы не отдельно, а как систему, приводит к выработке совокупности взглядов и оценок для общего случая на сущность проблем и общих решений. Одной из системообразующих задач является обоснованный выбор требуемого уровня защиты информации, поскольку как занижение, так и завышение уровня неизбежно ведет к потерям. В связи с этим чрезвычайно значимой является систематизация и обоснование создания условий, необходимых для оптимальной реализации концепции защиты [1, 2].

Системно-концептуальный подход, используемый в [1], получил дальнейшее развитие в [5], где выдвигается единая концепция защиты, основанная на комплексном применении всех имеющихся методов и средств, определяются основные требования к комплексным системам защиты информации, среди которых:

- использование комплекса программно-технических средств и организационных мер;
- надежность, производительность, конфигурируемость;
- экономическая целесообразность;
- возможность совершенствования;
- обеспечение разграничения доступа к конфиденциальной информации с отвлечением нарушителя на ложную информацию;
- взаимодействие с незащищенными компьютерными сетями по установленным для этого правилам разграничения доступа;
- обеспечение проведения учета и расследования случаев нарушения безопасности информации в компьютерных сетях и т.д.

Дальнейшее совершенствование теории защиты очевидно связано с учетом новых обстоятельств, характерных для современного периода развития информатизации общества:

- наблюдаемые в последние годы тенденции в развитии информационных технологий ведут к появлению качественно новых (информационных) форм борьбы, в том числе и на межгосударственном уровне. В силу этого все большую актуальность приобретает не только защита информации, но и защита людей и технических (главным образом, электронных) систем от разрушающего воздействия информации, в связи с чем формируется задача обеспечения информационной безопасности как органической совокупности задач защиты информации и защиты от информации;
- с самого начала регулярного использования автоматизированных технологий обработки информации актуальной является задача обеспечения требуемого качества информации. С течением времени актуальность данной задачи возрастает, а сама задача усложняется;
- основное внимание на новом этапе развития теории защиты информации должно быть уделено совершенствованию научно-методологического базиса и инструментальных средств, обеспечивающих решение любых возникающих задач на регулярной основе.

Углубленное изучение проблемы совершенствования научно-методологического базиса теории защиты информации привело к выводу, что уже в настоящее время и в перспективе решение проблем защиты вне органической связи с решением более общих проблем (информационных технологий, информатизации общества и т.д.) может привести к неадекватным результатам.

Цель стать и постановка заданий

До недавнего времени комплексные системы защиты информации были ориентированы на защиту информации, которая создается, редактируется и передается непосредственно в самой системе. Однако, существование и функционирование любой системы невозможно без коммуникации с внешней средой и другими системами. Таким образом, защищенность информации в самой системе будет зависеть от достоверности и целостности информации, поступающей извне. До недавнего времени методы проверки целостности не были учтены при построении классификации методов защиты информации.

Целью данной работы является построение новой классификации методов защиты информации с учетом методов проверки целостности цифровых сигналов.

Для достижения поставленной цели необходимо решить следующие задачи:

1) Рассмотреть существующие классификации методов защиты информации;
2) Определить основание для классификации на каждом уровне;
3) Провести классификацию методов проверки целостности цифровых сигналов.

Основная часть

Для решения задач защиты информации (ЗИ) существует целый ряд методов, которые, по способу их реализации были классифицированы следующим образом: организационные, технические, криптографические и программные [1,2].

Организационные методы защиты информации (МЗИ), в свою очередь, были разделены на законодательные [5–7], административные [8] и морально-этические методы, которые направлены на: использование законодательных актов, регламентирующих права и обязанности физических и юридических лиц, а также государства в области ЗИ; организацию соответствующего режима секретности, пропускного и внутреннего режима на объекте; создание и поддержание на объекте моральной атмосферы, в которой нарушение регламентированных правил поведения оценивалось бы большинством сотрудников резко негативно [1].

Технические методы включают в себя применение электронных и других устройств для ЗИ [9].

В *криптографических* методах используется шифрование и кодирование для сокрытия обрабатываемой и передаваемой информации от несанкционированного доступа [10,11].

Программные методы используют программные средства разграничения доступа к информации [5].

Представленные методы защиты информации нацелены на сохранение основных категорий информации – целостности, доступности, конфиденциальности, достоверности. Такие методы назовем методами *активной* защиты информации (МАЗИ).

В последние годы благодаря широкому распространению всевозможных средств (бытовых и специальных) фиксации и хранения фото-, видео- и аудиоинформации в распоряжении органов дознания, следствия и суда часто оказываются фотографии, видео- и аудиозаписи, которые могут являться доказательствами по уголовному делу.

Все чаще возникают следственные ситуации, в которых появляется необходимость в производстве экспертизы предоставленных материалов [12].

Для решения подобных задач применяются другие методы защиты информации (МЗИ), целью работы которых (в отличие от МАЗИ) является обоснованная констатация факта наличия или отсутствия нарушения одной или нескольких категорий информации, чаще всего целостности. Назовем их методами *пассивной* ЗИ (МПЗИ).

В качестве основания на первом уровне новой классификации предлагается использовать цель использования МЗИ, на втором – способ реализации (способ достижения цели) МЗИ. Схематически предложенная классификация методов защиты информации представлена на рисунке 2.

Методы защиты информации первоначально можно классифицировать по цели их использования на методы активной и пассивной защиты. Целью методов активной защиты информации является сохранение всех категорий информации. Методы пассивной защиты информации нацелены на то, чтобы дать ответ, было ли произведено преднамеренное нарушение какой-либо категории информации.

По способу реализации МАЗИ можно классифицировать в соответствии с [1, 2] на организационные, технические, криптографические и программные. МПЗИ по способу их реализации можно разделить на методы экспертной оценки, программно-технические и программные.

Методы *экспертной* оценки используют визуальное или акустическое оценивание информации специалистом. Главным недостатком методов экспертной оценки является наличие человеческого фактора.

Программно-технические МПЗИ основываются на знании специфических особенностей устройств аудио-, видео- или фотофиксации и (или) воздействия каких-либо внешних факторов на проведение записи.

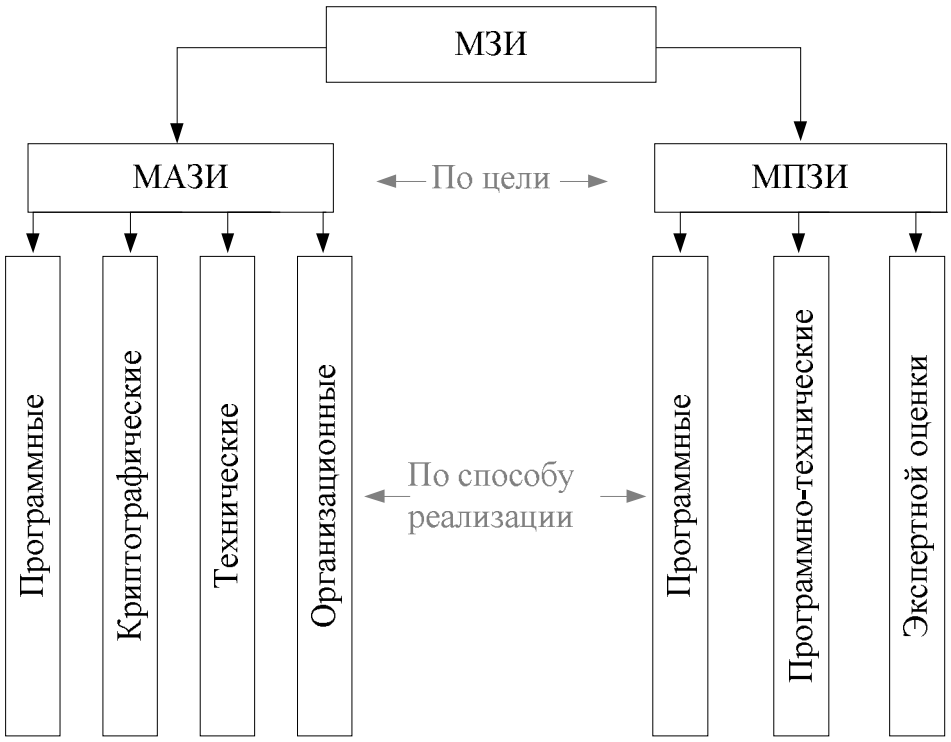

Рис. 2. Новая классификация методов защиты информации

Программные методы ЗИ анализируют лишь цифровую форму представления самого сигнала [13, 14], а поэтому не зависят от технических характеристик устройств или человеческого фактора, как в программно-технических методах и методах экспертного оценивания.

Выводы

В работе построена новая классификация МЗИ, которая более полно отражает существующие на сегодняшний день методы защиты информации, дает системное представление о способах их реализации и позволяет определить место методов проверки целостности цифровых сигналов среди всех остальных методов.

Предложенная классификация может быть полезна при изучении существующих и разработке новых методов и средств защиты информации.

Список литературы

1. Хорошко, В.А. Методы и средства защиты информации [Текст] : научное издание / В.А. Хорошко, А.А. Чекатков; Ред. Ю.С. Ковтанюк. — К. : ЮНИОР, 2003. — 505 с.
2. Ленков, С.В. Методы и средства защиты информации: в 2 т. / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. — К.: Арий, 2008 — . — Т.2: Информационная безопасность. — 2008. — 344 с.
3. Мамиконов, А.Г. Достоверность, защита и резервирование информации в АСУ [Текст] / А.Г. Мамиконов, В.В. Кульба, А.Б. Шелков. — М. : Энергоатомиздат, 1986. — 303 с.
4. Тихонов, А.Н. О состоянии работ по совершенствованию подготовки кадров по проблеме информационной безопасности / А.Н. Тихонов // Безопасность информационных технологий. — 1995. — № 4. — С. 43–52.
5. Хорев, П.Б. Методы и средства защиты информации в компьютерных системах [Текст] : учебное пособие для студентов вузов, обучающихся по спец. «Информатика и вычислительная техника» / П.Б. Хорев. — 2-е изд., стер. — М. : Изд. центр «Академия», 2006. — 256 с.
6. Чумарин, И.Г. Тайна предприятия: что и как защищать : учебное пособие / И.Г. Чумарин. — Санкт-Петербург : ДНК, 2001. — 160 с.
7. Стрельцов, А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы [Текст] : монография / А.А. Стрельцов ; Под ред. В.А. Садовничего, В.П. Шерстюка. — М. : МЦНМО, 2002. — 289 с.
8. Степанов, Е.А. Информационная безопасность и защита информации [Текст] : учеб. пособие / Е.А. Степанов, И.К. Корнеев. — М. : Инфра-М, 2001. — 302 с.
9. Хорев, П.Б. Способы и средства защиты информации / П.Б. Хорев. — М.: МО РФ, 2000. — 316 с.
10. Фергюсон, Н. Практическая криптография [Текст] : монография / Н. Фергюсон, Б. Шнайер ; Пер. с англ. Н.Н. Селиной. — М. и др. : ИД Вильямс : Диалектика, 2005. — 421 с.
11. Столингс, В. Криптография и защита сетей [Текст] : принципы и практика / Пер. с англ. А.Г. Сивака, А.А. Шпака; Под ред. А.Г. Сивака. — 2-е изд. — М. СПб. Киев : Вильямс, 2001. — 672 с.
12. Оленин, Г.В. Экспертиза цифровой аудио- и видеозаписи. Применение в следственной практике устройств цифровой фиксации аудио- и видеоинформации / Г.В. Оленин // Эксперт-криминалист. — 2009. — № 2. — С. 21–24.
13. Нариманова, Е.В. Исследование эффекта двойного квантования и его использование при обнаружении фальсификации ЦИ / Е.В. Нариманова // Вісник Східноукраїнського національного університету ім. В. Даля. — 2008. — № 8(126), Ч. 1. — С. 47–55.
14. Нариманова, Е.В. Практическое использование DQ-эффекта для построения универсального метода обнаружения фальсификации ЦС / Е.В. Нариманова // Вісник Східноукраїнського національного університету ім. В. Даля. — 2010. — № 9(151), Ч. 1. — С. 80–85.

НОВА КЛАСИФІКАЦІЯ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

О.В. Наріманова, К.О. Трифонова

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: semejka@ua.fm

Запропонована нова класифікація методів захисту інформації з урахуванням методів перевірки цілісності цифрових сигналів, які на сьогоднішній день викликають найбільший інтерес, проте не мають свого місця в рамках методів та засобів захисту інформації.

Ключові слова класифікація, методи захисту інформації, методи перевірки цілісності, методи активного захисту інформації, методи пасивного захисту інформації

A NEW CLLASSIFICATION OF INFORMATION PROTECTION METHODS

Olena V. Narimanova, Ekaterina A. Trifonova

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: semejka@ua.fm

A new classification of information protection methods including methods of digital signals integrity check is proposed. The last ones today are the most popular but do not have their place among the information protection methods.

Keywords: classification, information protection methods, methods of integrity check, methods of active information protection, methods of passive information protection