2. ГОСТ Р 55062-2012 «Системы промышленной автоматизации и их интеграция. Интероперабельнсть . Основные положения.

3. Куделькин В.А., Денисов В.Ф. Модели и инструментальные средства мониторинга состояния комплексной безопасности стратегических объектов и территорий.// журнал «Мониторинг. Наука и безопасность.» -М., 2012, №2 (6), с. 16-24.

4. Куделькин В.А., Денисов В.Ф. Архитектура интегрированных распределенных систем мониторинга и обеспечения безопасности организационно-технических систем и территорий.// Мониторинг.Наука и безопасность», 2013, №4 (12), с. 64-79.

5. Куделькин В.А., Денисов В.Ф. Организационно-методическое обеспечение и стандартизация интегрированных систем мониторинга и обеспечения безопасности стратегических и социально значимых объектов и территорий государства// Журн. Интеграл, № 1 (74), 2014 г, с.50-52.

6. ISO/IEC DIS 18384-3 Distributed Application Platforms and Services (DAPS)-Reference Architecture for Service Oriented Architecture(SOA). Part 3:Service Oriented Architecture Ontology (draft international standard)

Е.Г. Загузина

## ПОСТРОЕНИЕ ФУНКЦИИ РАБОТОСПОСОБНОСТИ ПРИ ОЦЕНКЕ «ЖИВУЧЕСТИ» СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

(Санкт-Петербургский государственный экономический университет)

В условиях информационной экономики одним из актуальных вопросов является сохранение информационной безопасности государства. Информационная безопасность является основной составляющей национальной безопасности. Условием информационной безопасности является наличие системы защиты информации (СЗИ), представляющей собой в широком смысле сложно структурированную систему, работа которой направлена на защиту критической инфраструктуры государства. В более узком смысле СЗИ представляет собой комплекс организационных и технических мер, направленных на обеспечение информационной безопасности. Главным объектом защиты являются данные, которые обрабатываются в автоматизированной системе управления (АСУ) и задействованы при выполнении бизнес-процессов.

Как любая другая система, СЗИ должна обладать основными свойствами системы, обеспечивающими работу системы в целом и ее элементов. Одна из форм свойства устойчивости (способности противостоять разрушающим систему воздействиям) является свойство «живучесть», которое определяется работоспособностью системы. Термин «живучесть» заимствован из терминологии биологических систем.

Живучесть СЗИ представляет собой способность системы сохранять и восстанавливать выполнение основных функций в заданном объеме и на протяжении заданного времени в случае изменения структуры системы и/или алгоритмов и

условий ее функционирования вследствие неблагоприятных воздействий [1, С. 20-23].

Свойство живучести для СЗИ является наиболее важным в сравнении с другими системами, поскольку от наличия данного признака зависит не только функционирование самой СЗИ, но и работа тех объектов, на которые направлена ее защита. Нарушение работы СЗИ влечет за собой появление каналов утечки информации, и, следовательно, негативных последствий в целом для объекта защиты.

Наиболее приемлемым методом анализа живучести сложно структурированных систем является логико-вероятностный метод (ЛВМ) [2, С. 54].. В рамках данного метода на этапе постановки задачи анализа используются схемы функциональной целостности (СФЦ), предназначенные для строго формализованного представления общей логической организации взаимного функционирования всех элементов системы в целом.

Так, в качестве примера приведена примитивная СЗИ, построенная на основе аутентификации пользователей информационной системы, с криптографическим закрытием хранимых и передаваемых по каналам связи данных. На рис. 1 показан граф связности рассматриваемой СЗИ, на рис. 2 ее СФЦ.

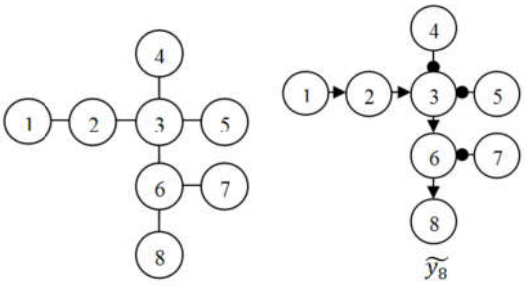


Рис 1. Граф связности (слева) и СФЦ СЗИ (справа)

Действие примитивной СЗИ можно описать следующей цепочкой событий информационной системы: 1 – запрос пользователя на получение информации; 2 – запрос пользователя на подтверждение подлинности (аутентификация); 3 – обработка запроса на получение доступа блоком управления; 4 – подтверждение подлинности (аутентификация); 5 – согласие на передачу запрашиваемой информации из базы данных; 6 – криптографическое шифрование данных; 7 – введение пользователем криптографического ключа; 8 – передача информации в блок ввода-вывода информации.

Рассмотренную систему можно отнести к классу монотонных систем. Получение информации на блок ввода-вывода возможно только при успешном прохождении аутентификации и введения правильного криптографического ключа пользователем. Таким образом, логический критерий целостности (ЛКЦ) представлен в виде:

$$Y_c = y_8 \quad (1)$$

При этом общий отказ системы определится одновременной функциональной неработоспособностью элементов 4, 5 и 7:

$$\overline{Y_c} = \overline{y_4} \cdot \overline{y_5} \cdot \overline{y_7} \quad (2)$$

Построим искомую функцию работоспособности системы (ФРС):

$$\overline{Y_c} = x_8 \cdot [x_6 \cdot [x_3 \cdot [x_2 \cdot x_1] \cdot (x_4 \cdot x_5) \cdot x_7] \quad (3)$$

Рассмотренная примитивная СЗИ будет работать только в случае работоспособности всех элементов и совершения заданных событий. Модифицируя СФЦ, можно получить несколько сценариев исполнения основных функций СЗИ – начиная режимом полного функционирования до режима аварийной работы.

Таким образом, на данном этапе оценки «живучести» СЗИ была получена математическая модель функционирования элементов системы.

**Литература**

1. Можаев А.С. Теоретические основы общего логико-вероятностного метода автоматизированного моделирования систем / А. С. Можаев, В. Н. Громов. – СПб. : ВИТУ, 2000. – 145 с.

2. Синтез и анализ живучести сетевых систем : монография / Ю.Ю. Громов, В. О. Драчев, К. А. Набатов, О. Г. Иванова. – М. : «Издательство Машиностроение-1», 2007. – 152 с.

А.В. Киселева, М.А. Кудрина

## СТЕГАНОГРАФИЯ И МЕТОДЫ СТЕГОАНАЛИЗА

(Самарский национальный исследовательский университет
имени академика С.П. Королева)

Стеганографическая система или стегосистема – совокупность средств и методов, которые используются для формирования скрытого канала передачи информации [1]. В качестве данных может использоваться любая информация: текст, сообщение, изображение и т. п.

Контейнер – любая информация, предназначенная для сокрытия тайных сообщений.

По используемому принципу скрытия методы компьютерной стеганографии делятся на два основных класса: методы непосредственной замены и спектральные методы. Если первые, используя избыток информационной среды, заключаются в замене малозначительной части контейнера битами секретного сообщения, то другие для скрытия данных используют спектральные представления элементов среды, в которую встраиваются скрываемые данные.

В рассматриваемой системе были реализованы следующие методы стеганографии: метод замены наименьших значащих битов или LSB-метод, метод Куттера-Джордана-Боссена, метод Коха-Жао, а так же метод скрытой передачи цветных изображений bmp.

Стегоанализ – наука о выявлении факта передачи скрытой информации в анализируемом сообщении. В некоторых случаях под стегоанализом понимают также извлечение скрытой информации из содержащего её сообщения и (если это необходимо) дальнейшую её дешифровку [2].