DOI: 10.17117/na.2014.01.181

Поступило в редакцию: 12.11.2014

<http://ucom.ru/doc/na.2014.01.181.pdf>**Говорухина Т.Н., Михайлов А.В.****Методика построения имитационных моделей защиты информации в каналах передачи данных телеметрических систем****Govorukhina T.N., Mikhaylov A.V.****Method of constructing simulation models of information security in data transmission channels of telemetry systems**

Рассматривается методический подход к анализу возможностей информационной защиты больших многоуровневых телеметрических систем, содержащих внешние и внутренние каналы и средства обмена и передачи данных пользователям

Ключевые слова: имитационная модель, телеметрическая система, защита информации

Говорухина Татьяна Николаевна

*Кандидат технических наук, преподаватель
Юго-Западный государственный университет
г. Курск, ул. 50 лет Октября, 94*

Михайлов Алексей Владимирович

*Аспирант
Юго-Западный государственный университет
г. Курск, ул. 50 лет Октября, 94*

Considers methodical approach to the analysis of information security capabilities of large multi-level telemetry systems containing internal and external channels and means of exchange and data users

Key words: simulation model, telemetry system, information security

Govorukhina Tatiana Nikolaevna

*Candidate of Technical Sciences, Lecturer
Southwestern State University
Kursk, 50 years October st., 94*

Mikhaylov Alexey Vladimirovich

*Postgraduate
Southwestern State University
Kursk, 50 years October st., 94*

ВВЕДЕНИЕ.

Семантически понятие «информация» трактуется [1] как сведения (данные), отраженные на каком-либо материальном носителе и используемые в целях получения знаний и принятия практических решений (в том числе – управляющих и управленческих). Эти сведения, в том числе на высоком уровне порождает телеметрическая система (ТМС) как структурно и функционально упорядоченная совокупность информационных ресурсов, соответственно отображаемых на технической структуре [2, 3] средств, технологий и алгоритмов, созданных и реализующих целенаправленные информационные процессы (ЦИП) для пользователей различного ранга.

Целевым фактором анализа является определение ценности и уязвимости информации, подлежащей защите, определения возможности угроз и ущерба.

Ценность информации определяется здесь через вероятность достижения цели (по Вудворду). Ценность внешней информации – привнесённой извне и способной к самосохранению, а также – увеличению влияния на перспективу системы в целом.

Ценность информации J возрастает с увеличением ее влияния на вероятность события, которое она представляет, т.е.

$$J = \frac{V_0}{V_1}, \quad (1)$$

где V_0 – число возможных исходов до получения информации,

V_1 – число возможных исходов после получения информации.

Всестороннее оценивание позволяет определить состав и сопоставительную цену усилий по защите полученной информации на всех этапах её преобразования и обработки. Искажения данных или формирование заведомо ложных сообщений пользователем может породить ошибки, цена которых может оказаться очень большой.

ПОСТАНОВКА ЗАДАЧИ.

Информационная безопасность является достаточно сложной и многогранной проблемой, для решения которой должна быть сформирована соответствующая теоретическая и практическая база, комплекс подходов, методик и необходимых функционально-структурных организаций, предполагающих:

- определение функционального и структурного состава ТМС и её внутренних и внешних информационных каналов, в том числе – «паразитных» (непреднамеренных);
- анализ и имитация свойств предполагаемого состава уязвимых компонентов как самой ТМС, так и её периферийной информационной сети;
- оценивание угроз (выявления проблемных факторов, имеющих место из-за наличия выявленных уязвимых компонентов);
- анализ и имитация рисков (раннее прогнозирование возможных последствий преднамеренного и непреднамеренного искажения информации);
- составление перечня угроз, которые необходимо устранить, определение направлений и возможных способов их устранения;
- формирование перечня информационных ресурсов, подлежащих защите;
- определение состава и структуры методов и средств, позволяющих реализовать саму защиту;
- определение потенциальных затрат, допустимых при решении задачи защиты.

РЕШЕНИЕ ЗАДАЧИ

Информация как продукт ТМС, изменяет информационные свойства согласно принятой технологии (алгоритму) посредством совокупности определенным образом организованных технических средств и операторов, представляющих стандартные и специализированные операции.

Фигурантами обмена являются:

- информационный ресурс;
- оператор (пользователь);

– ТМС (оператор посредник).

Полнота ликвидации угроз возможна при рассмотрении и учете всех компонентов формирования и обмена информацией, в том числе – элементов периферий ТМС (рисунок 1).

Информационное взаимодействие ТМС представляет собой, по сути, информационный конфликт, где целью объектовой стороны является минимизация возможности искажения (или утечки) информации, с одной стороны, а с другой – возможность воздействия комплекса мешающих факторов различного характера.

Рис 1. Вербальная модель информационного взаимодействия ТМС внутреннего и внешнего порядка

Методика оценивания возможностей информационной защиты многоуровневой ТМС определяется в основном, за счёт локальных моделей, в совокупности отражающих главные аспекты оптимизации (или рациональности) решения поставленных задач.

Основным инструментом построения моделей рассматриваемых процессов является использование способов и приемов формализации информационных процессов и их защиты на всех уровнях иерархии решаемых задач.

Нижней стратой (первичная обработка) считается получение сигналов от датчиков, измерение их параметров, формирование оценок и выбор информативных признаков при мониторинге и контроле технологических процессов и объектов.

Средний уровень – сортировка и подготовка данных, внутренние перемещения информации.

Верхней стратой считается реализация алгоритмов вторичной обработки измерительной и известительной информации, выбор критериев распознавания ситуаций, их идентификация и прогнозирование развития.

Методика первого этапа защиты ТМС в информационном плане предполагает реализацию процедуры оценивания потенциальной возможности искажения и утечки информации, на базе чего (согласно принципу гарантированности) синтезируется набор правил и моделей устранения (уменьшения) угроз.

Список литературы:

1. Александров Е.А. Основы теории эвристических решений. М.: Сов. Радио, 1975. 256 с.
2. Бурмака А.А., Левченко А.В., Фишер И.В. Архитектура и системная модель информационно-измерительных систем многофакторного мониторинга // Системный анализ в биомедицинских системах, 2011 Т. 10. №4. С. 884-888.
3. Бурмака А.А., Левченко А.В., Фишер И.В. Архитектура информационно-измерительных систем многофакторного мониторинга для конфигураций открытого типа // Медико-экологические информационные технологии-2009. С. 310-318.
4. Охтилев М.Ю., Юсупов Б.В., Юсупов Р.М. Интеллектуальные технологии мониторинга и управления структурной динамикой сложных технических объектов. М.: Наука, 2006. 405 с.

© 2014, Говорухина Т.Н., Михайлов А.В.
*Методика построения имитационных моделей
защиты информации в каналах передачи данных
телеметрических систем*

© 2014, Govorukhina T.N., Mikhaylov A.V.
*Method of constructing simulation models of
information security in data transmission channels
of telemetry systems*