# Table of Contents

## Invited Talks

An Intelligent Decision Support System for Intrusion Detection and Response ........................................................... 1  
*Dipankar Dasgupta, Fabio A. Gonzalez*

Mathematical Models of the Covert Channels ........................... 15  
*Alexander Grusho*

Open Issues in Formal Methods for Cryptographic Protocol Analysis ... 21  
*Catherine Meadows*

Future Directions in Role-Based Access Control Models ................. 22  
*Ravi Sandhu*

Secure Networked Computing ........................................... 27  
*Vijay Varadharajan*

## Network Security Systems: Foundations, Models, and Architectures

Composability of Secrecy ............................................... 28  
*Jan Jürjens*

Agent-Based Model of Computer Network Security System: A Case Study 39  

Security Considerations and Models for Service Creation in Premium IP Networks ........................................... 51  
*Michael Smirnov*

Secure Systems Design Technology ...................................... 63  
*Peter D. Zegzhda, Dmitry P. Zegzhda*

A Privacy-Enhancing e-Business Model Based on Infomediaries .......... 72  
*Dimitris Gritzalis, Konstantinos Moulinos, Konstantinos Kostis*

Applying *Practical* Formal Methods to the Specification and Analysis of Security Properties ...................... 84  
*Constance Heitmeyer*

Modeling Software Tools Complex for Evaluation of Information Systems Operation Quality (CEISOQ) .......................... 90  
*Andrey Kostogryzov*

Analyzing Separation of Duties in Petri Net Workflows ............... 102  
*Konstantin Knorr, Harald Weidner*
### Intrusion Detection: Foundations and Models

Information Security with Formal Immune Networks .......................... 115  
*Alexander O. Tarakanov*

BASIS: A Biological Approach to System Information Security .......... 127  
*Victor A. Skormin, Jose G. Delgado-Frias, Dennis L. McGee,  
Joseph V. Giordano, Leonard J. Popyack, Vladimir I. Gorodetski,  
Alexander O. Tarakanov*

Learning Temporal Regularities of User Behavior for Anomaly Detection 143  
*Aleksandr Seleznyov, Oleksiy Mazhelis, Seppo Puuronen*

Investigating and Evaluating Behavioural Profiling  
and Intrusion Detection Using Data Mining .............................. 153  
*Harjot Singh, Steven Furnell, Benn Lines, Paul Dowland*

### Access Control, Authentication, and Authorization

Typed MSR: Syntax and Examples ......................................... 159  
*Iliano Cervesato*

TRBACN: A Temporal Authorization Model ............................. 178  
*Steve Barker*

The Set and Function Approach to Modeling Authorization  
in Distributed Systems .................................................. 189  
*Tatyana Ryutov, Clifford Neuman*

Fenix Secure Operating System: Principles, Models, and Architecture ... 207  
*Dmitry P. Zegzhda, Pavel G. Stepanov, Alexey D. Otavin*

### Cryptography and Steganography: Mathematical Basis, Protocols, and Applied Methods

Generalized Oblivious Transfer Protocols Based on Noisy Channels...... 219  
*Valeri Korjik, Kirill Morozov*

Controlled Operations as a Cryptographic Primitive .................... 230  
*Boris V. Izotov, Alexander A. Moldovyan, Nick A. Moldovyan*

Key Distribution Protocol Based on Noisy Channel  
and Error Detecting Codes ............................................ 242  
*Viktor Yakovlev, Valery Korjik, Alexander Sinuk*

Dynamic Group Key Management Protocol ............................... 251  
*Ghassan Chaddoud, Isabelle Chrisment, André Schaff*

SVD-Based Approach to Transparent Embedding Data  
into Digital Images ..................................................... 263  
*Vladimir I. Gorodetski, Leonard J. Popyack, Vladimir Samoilov,  
Victor A. Skormin*

Fast Encryption Algorithm Spectr-H64 .................................. 275  
*Nick D. Goots, Alexander A. Moldovyan, Nick A. Moldovyan*
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVS at Work: A Report on New Failures upon Some Cryptographic Protocols</td>
<td>287</td>
</tr>
<tr>
<td>Antonio Durante, Riccardo Focardi, Roberto Gorrieri</td>
<td></td>
</tr>
<tr>
<td>On Some Cryptographic Properties of Rijndael</td>
<td>300</td>
</tr>
<tr>
<td>Selçuk Kavut, Melek D. Yücel</td>
<td></td>
</tr>
<tr>
<td><strong>Author Index</strong></td>
<td>313</td>
</tr>
</tbody>
</table>