



**ЎАЛҚАРО ИЛМИЙ КОНФЕРЕНЦИЯСИ  
МЕЖДУНАРОДНАЯ НАУЧНАЯ КОНФЕРЕНЦИЯ**

**ФАН, ТЕХНИКА ВА ТАЪЛИМДА  
ИНФОКОММУНИКАЦИОН ВА ҲИСОБЛАШ  
ТЕХНОЛОГИЯЛАРИ**

2004 йил 28–30 сентябр, Тошкент ш.

**ИНФОКОММУНИКАЦИОННЫЕ  
И ВЫЧИСЛИТЕЛЬНЫЕ ТЕХНОЛОГИИ В  
НАУКЕ, ТЕХНИКЕ И ОБРАЗОВАНИИ**

28–30 сентября 2004 года, г. Ташкент

Ўалқаро конференция маърузалари ва тезислари  
Доклады и тезисы международной конференции

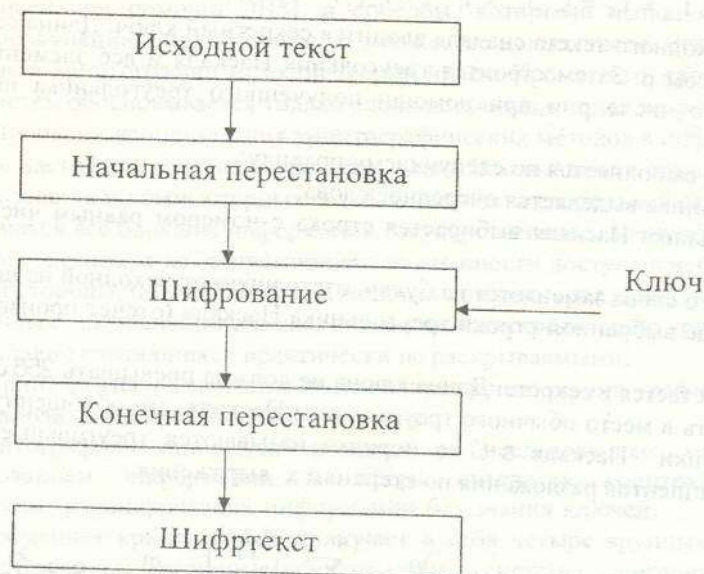
Тошкент – 2004 – Ташкент

## СЕКЦИЯ: ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ И СЕТЯХ

Абдукаюмов А., Ташходжаева Н.С. «Проблема защиты информации в автоматизированных системах».....	551
Адылова З.Т., Игнатьев Н.А, Мадрахимов Ш.Ф. «Методы защиты информации в компьютерных сетях, основывающиеся на многоагентных технологиях».....	554
Алиев Д.В. «Области применения биометрических систем».....	559
Ганиев С.К, Каримов М.М., Эшанкулов Т.Н. «К вопросу аппаратного шифрования данных».....	563
Касымов С.С. «Подготовка кадров в области информационной безопасности».....	566
Мухамадиева К. Б. «Некоторые методы защиты информации в сети internet».....	570
Назиров Ш.А. Бабакулов И.Х. «К вопросам разработки алгоритмов и программного обеспечения шифрования информации».....	571
✓ Позиллов М.С., А.С.Байдуллаев. «О моделирование систем информационной безопасности».....	574
✓ Позиллов М.С., Ибрагимов И.И., Тошбоев С.Д. «Информацион глобаллашув шароитида ахборот оқими Ўзбекистон миллий хавфсизлиги таҳдид сифатида».....	577
Шишкин В.М., Юсупов Р.М. «Аксиоматическое определение основных понятий информационной безопасности».....	583
Юлдашев М.Д. «Маълумотлар узатиш тармоқларида ахборотни тўлиқлигини таъминлашда «Электрон рақамли имзониинг ўрни».....	587

### СМЕШАННАЯ СЕКЦИЯ

Отакулов С., Азизов И. «Математическая модель задачи оптимального управления для системы с запаздыванием и параметром неконтролируемых внешних воздействий»	589
Паршиев А., Аллаёров С., Абдурахимов Д. «Компьютер ва ахборот-коммуникация технологиялар имкониятларидан фойдаланиш»	592
Мирзаев Ч.Э., Аллаёров С.П. «Таълимда янги педагогик технологиялар ва унинг муаммолари»	594
Аллаёров С.П., Абдурахимов Д.Б., Жураев У.С. «Основные принципы безопасности программного обеспечения»	598



В настоящее время по заданной схеме шифрования на основе треугольника Паскаля разработана программное средства в среде Borland Delphi 6.0.

#### Литература

1. Бондаренко Б.А. Обобщенные треугольник и пирамиды Паскаля, их фракталы, графы и приложения. Ташкент. Фан. 19 с.
2. Романец Ю.В., Тимофеев П.А., Шаньгин В.Д., Защита информации в компьютерных системах и сетях. М: Радио и связь, 2001.-376 стр.

### О МОДЕЛИРОВАНИЕ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Пазылов М.С., Байдуллаев А.С.

Ташкентский фармацевтический институт, Ташкент, M\_Pozilov@rambler.ru

Фактически моделирование т.е. построение и исследование моделей есть некий инструмент исследования реальных систем и происходящих в них процессов путем воспроизведения их характеристик на искусственных объектах (моделях), которые специально созданы для их изучения. Модели систем информационной безопасности (СИБ) входят в научно-методологический и инструментальный базис теории защиты информации и информационной безопасности.

Как правило, суть моделирования сводится к решению двух основных задач:

1. Оценка текущих характеристик и параметров региональных систем информационной безопасности (РСИБ),
2. Прогнозирование их будущего поведения.

На основе результатов моделирования строятся стратегии безопасности и механизмы их реализации, которые составляют основу создания, функционирования и развития РСИБ. Их совокупность является базовым набором подобных систем и не переменным условием устойчивого развития как РСИБ, так и рассматриваемого регионального информационного пространства.

Чаще всего задачи классифицируются исходя из моделируемой ситуации, которая может состоять в следующем:

- создание СИБ;
- совершенствование СИБ;
- управление СИБ.

В общем случае, сам процесс можно разделить на две составляющие:

- построение модели,
- реализация модели с целью получения необходимых характеристик системы.

Как для первого, так и для второго подхода необходима классификация моделей, которую уместно осуществить с учетом основных задач моделирования применительно к РСИБ.

Классификация моделирования СИБ может осуществляться по совокупности следующих признаков:

1) **способ моделирования**, т.е. тот базовый прием, который положен в основу построения модели. По этому критерию все модели могут быть разделены на:

- **аналитические** □ моделируемая система представляется в виде совокупности аналитических и/или логических зависимостей, позволяющих определять необходимые характеристики путем проведения вычислений по указанным зависимостям;

- **статистические** □ моделируемая система представляется в виде некоторого аналога, отражающего для определяемых характеристик зависимости реальной системы. Само определение значений этих характеристик осуществляется путем многократной имитации реализации зависимостей характеристик от существенно значимых параметров реальной системы и внешней среды, а также статистической обработки совокупности получаемых при этом результатов;

2) **характер моделируемой системы**, причем наиболее важным показателем этого критерия является характер взаимосвязей между подлежащими определению на модели значениями характеристик моделируемой системы и влияющими на них параметрами системы и внешней среды. По этому признаку моделируемые системы делятся на:

- **детерминированные** □ все зависимости строго и однозначно определены;

- **стохастические** □ на все зависимости оказывают существенное влияние случайные факторы;

3) **масштаб моделирования**, причем этот масштаб задается главным образом уровнем определяемых на модели характеристик. По данному критерию модели можно разделить на:

- **общие** □ модели, которые строятся с целью определения значений некоторых обобщенных характеристик моделируемых систем;

- **частные** □ модели, которые строятся с целью определения значений частных, локальных характеристик системы.

Процессы обеспечения информационной безопасности в значительной степени определяют многие факторы. Отсюда их модели могут быть стохастическими. Это сужает границы классификации и анализа, так как достаточно иметь в виду только четыре разновидности моделей (рис.1.).

В аналитических моделях структура моделируемых систем и процессы их функционирования представляются в неявном виде.

При статистическом моделировании системы структура адекватно отображается в модели, а процессы ее функционирования проигрываются (имитируются) на построенной модели. При этом степень адекватности модели реальной системе и процессов имитации на модели реальным процессам функционирования моделируемой системы определяется

целями моделирования, т.е. теми характеристиками системы, которые должны быть получены в процессе моделирования. Определяемые в процессе моделирования значения характеристик должны соответствовать значениям этих характеристик, которые будут и/или могут иметь место в процессе функционирования реальной системы.



Рис. 1. Разновидности моделей систем информационной защиты

Формирование статистической модели заключается в описании структуры и процессов функционирования системы, а имитация процессов функционирования — в проигрывании тем или иным способом смены во времени состояний модели системы и принятии на каждом шаге имитации тех решений, которые обусловлены сложившейся ситуацией и правилами функционирования реальной системы.

Описание структуры моделируемой системы может быть осуществлено элементами математического аппарата, а конкретнее — методами теории графов [1]. Описание же структуры моделируемой системы должно содержать:

- перечень и структуру всех значимых элементов системы;
- взаимные связи между элементами систем;
- характер этих взаимосвязей.

Как известно, и в теории графов имеются средства для представления всех трех перечисленных компонентов описания систем.

Значительное число параметров СИБ имеют «нечеткую природу» и носят неформальный характер. Оценки параметров являются экспертными.

Очевидная потребность рассмотрения динамического поведения систем делает перспективной для приложения в данной области методологии ситуационного моделирования с использованием объектно-ориентированного моделирования (ООМ).

1. Описание моделируемой системы (внутренней структуры системы и выполняемых ее компонентами преобразований), их статических и динамических связей. Описание внешней среды, в которой действует моделируемая система (ограничения). Описание системы управляющих воздействий (динамические воздействия и условия). Описание защищаемых ресурсов. При этом под объектом будем понимать некоторую элементарную компоненту из универсального набора с постоянной динамической структурой и функциональностью. Компоненты являются фреймами и объектами в языке. Описание системы является декларативным. Профили «нечеткие ограничения (в общем случае тоже фреймы).

2. Компиляция или интерпретация описаний в компьютерную модель.

3. Проведение экспериментов в соответствии с разработанным планом моделирования и обработка результатов экспериментов.

При этом можно выделить следующие группы первоочередных проблем:

- создания языка многоуровневого описания моделируемых систем (статике и динамике) и как важнейшей составляющей - формального описания защищаемых ресурсов;

- трансформации, с помощью трансформационных грамматик, разноуровневых моделей, описанных средствами различных языков.

Характерно отметить, что одним из наиболее общих и в тоже время инженерных языков в данном случае является описание систем информационной безопасности топологическими методами, учитывающими структурные особенности формируемых и развиваемых систем. Использование топологической методологии позволяет выделить главные факторы. Топологические преобразования являются самыми значимыми (критичными) в многофакторных РСИБ. На их основе можно наглядно учитывать многочисленные процедуры генерации, обработки и передачи информации в региональном информационном пространстве.

Под общими моделями систем и процессов защиты информации понимают те модели, которые позволяют определять или оценивать общие характеристики указанных систем. Локальные и частные модели, в свою очередь, обеспечивают определение или оценку некоторых локальных или частных характеристик систем или процессов.

Основное назначение общих моделей – создание предпосылок для объективной оценки общего состояния систем с точки зрения меры уязвимости или уровня защищенности. Необходимость в таких оценках обычно возникает при анализе общей ситуации с целью выработки стратегических решений при организации защиты информации, т.е. в процессе моделирования.

*Общая модель процесса обеспечения информационной безопасности* в самом общем виде и для самого общего объекта защиты должна отображать процесс взаимодействия дестабилизирующих факторов, воздействующих на информационный объект и средств защиты препятствующих действию этих факторов. Результатом взаимодействия будет тот или иной уровень информационной защищенности объекта.

*Обобщенная модель СИБ*, являясь дальнейшим развитием общей модели, должна отображать основные процессы, осуществляемые в ней с целью рационализации механизмов защиты. Указанные процессы в самом общем виде могут быть представлены как процессы распределения и использования ресурсов, выделяемых на обобщение информационной безопасности.

*Модель общей оценки информационных угроз* предусматривает оценку не только угроз как таковых, но и оценку ущерба, который может иметь место при проявлении данных угроз. Они важны еще и тем, что именно на них в наибольшей степени были выявлены те условия, при которых такие оценки могут быть адекватны реальным процессам обеспечения информационной безопасности.

#### Литература

- 1.Абалмазов Э.И. Методы и инженерно-технические средства противодействия информационным угрозам. М.: Гротек, 1997. □200 с.
- 2.Алексеев В.Н. Современная концепция комплексной защиты. Технические средства защиты. М.: АО «Ноулидж экспрес» и МИФИ, 1994. □100 с.

ИНФОРМАЦИОН ГЛОБАЛЛАШУВ ШАРОИТИДА АХБОРОТ ОҚИМИ  
ЎЗБЕКИСТОН МИЛЛИЙ ХАВФСИЗЛИГИГА ТАҲДИД СИФАТИДА

Позилев М.С., Ибрагимов И.И., Тошбоев С.Д.

Тошкент фармацевтика институти, Тошкент, M\_Pozilov@rambler.ru

Ҳозирги замон жамиятлари тараққиётининг сўнгги босқичи шахс, жамият, давлатнинг ҳаёти ва фаолиятига борган сари информацион соҳанинг таъсири кучайиши билан белгиланади. Информацион соҳа, яъни ахборотлар мажмуаси, маълумот ва ахборотни йиғувчи, тарқатувчи субъектлардан иборат тизим шак –