



НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ ЭКОНОМИКИ И УПРАВЛЕНИЯ «НИНХ»



Кафедра информационной безопасности

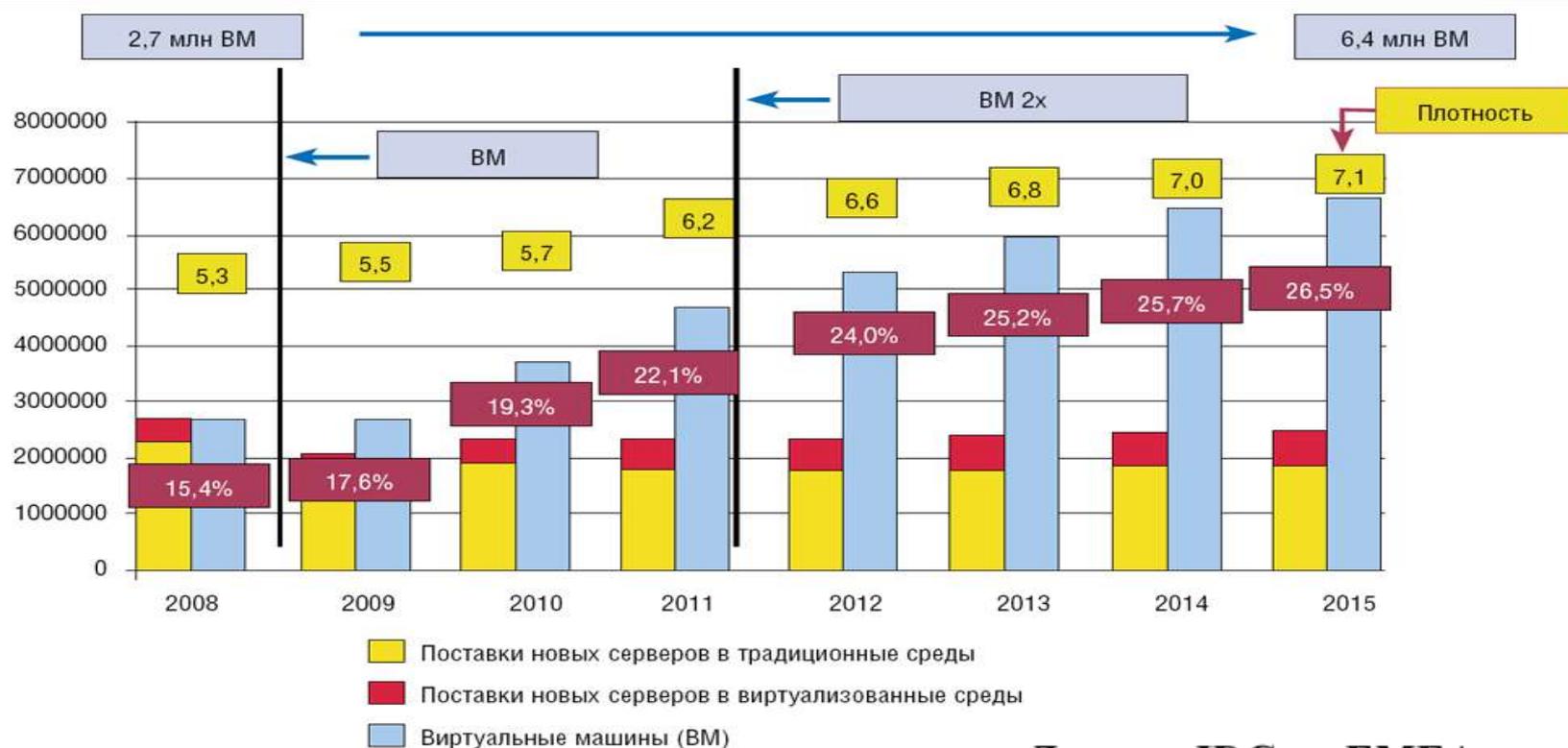
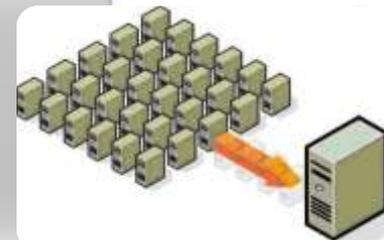
Модель идентификации угроз виртуальной инфраструктуры

Курносков Кирилл Викторович, *аспирант*

Пестунова Тамара Михайловна, *к.т.н., доцент*

Актуальность технологий виртуализации

- оптимальное использование вычислительных ресурсов;
- экономия физических ресурсов;
- новый уровень масштабируемости и расширяемости инфраструктуры;
- повышение уровня отказоустойчивости.



Данные IDC по EMEA

Задача обеспечения безопасности информации



Создание и поддержание в актуальном состоянии системы защиты информации, способной противодействовать актуальным угрозам безопасности информации, в том числе специфичным для среды виртуализации (с учетом требований обязательной и рекомендательной нормативно-методической базы)

Основные нормативно-методические требования и рекомендации:

- Приказ ФСТЭК России №17
- Приказ ФСТЭК России №21
- ГОСТ Р 56938-2016. Защита информации. Защита информации при использовании технологий виртуализации. Общие положения.
- Проект методики определения угроз безопасности информации в информационных системах

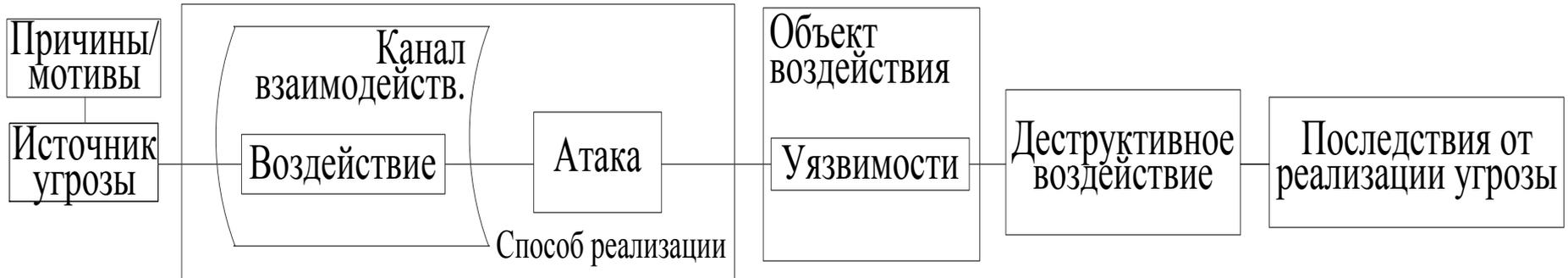
Задача идентификации угроз

Угроза безопасности информации - совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Атрибуты идентифицированной угрозы:

- источник угрозы (нарушитель);
- уязвимость;
- способ реализации;
- объект воздействия;
- последствия.

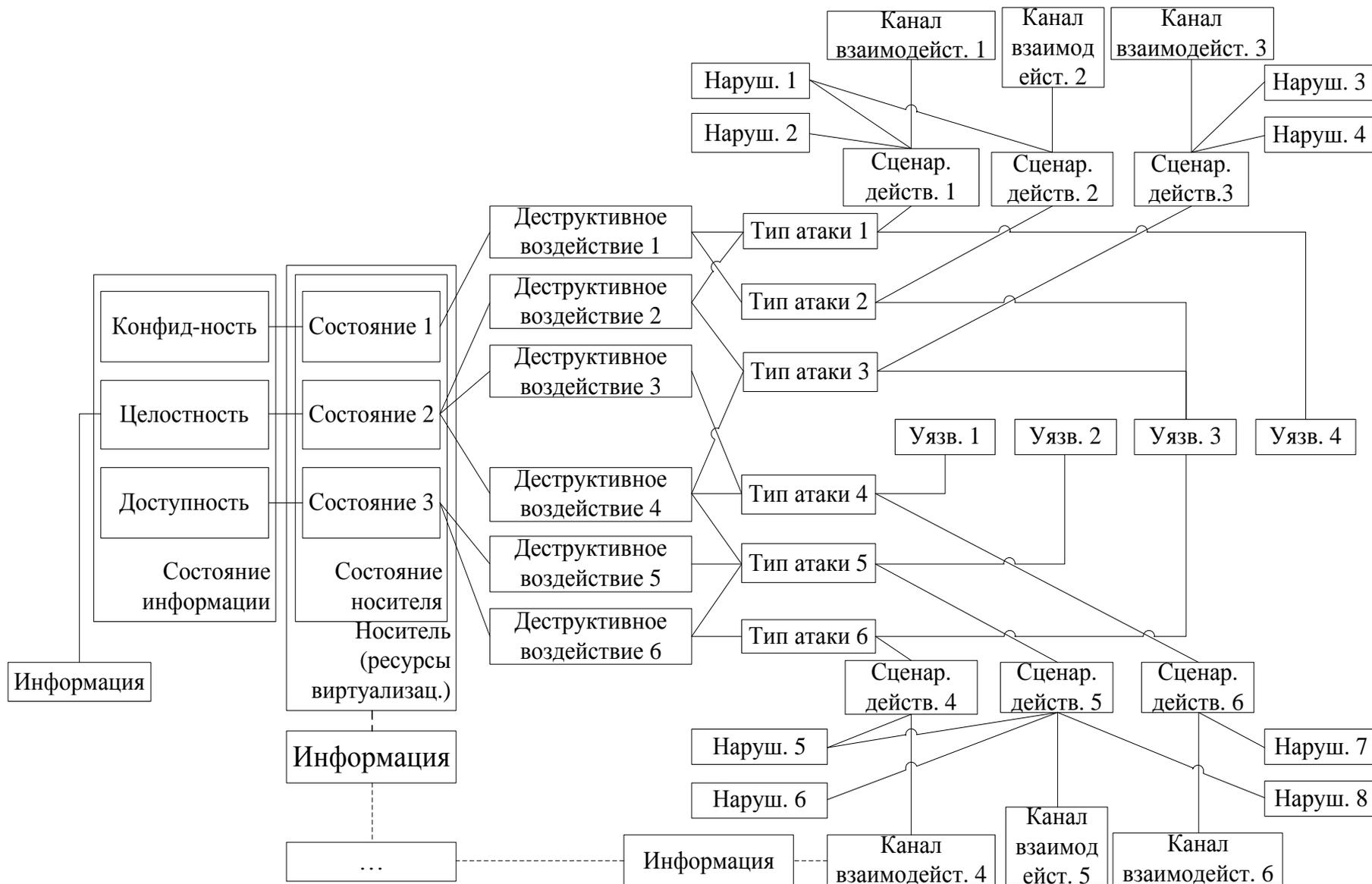
Задача идентификации угроз



Атрибуты идентифицированной угрозы:

- источник угрозы (нарушитель);
- уязвимость;
- способ реализации;
- объект воздействия;
- последствия.

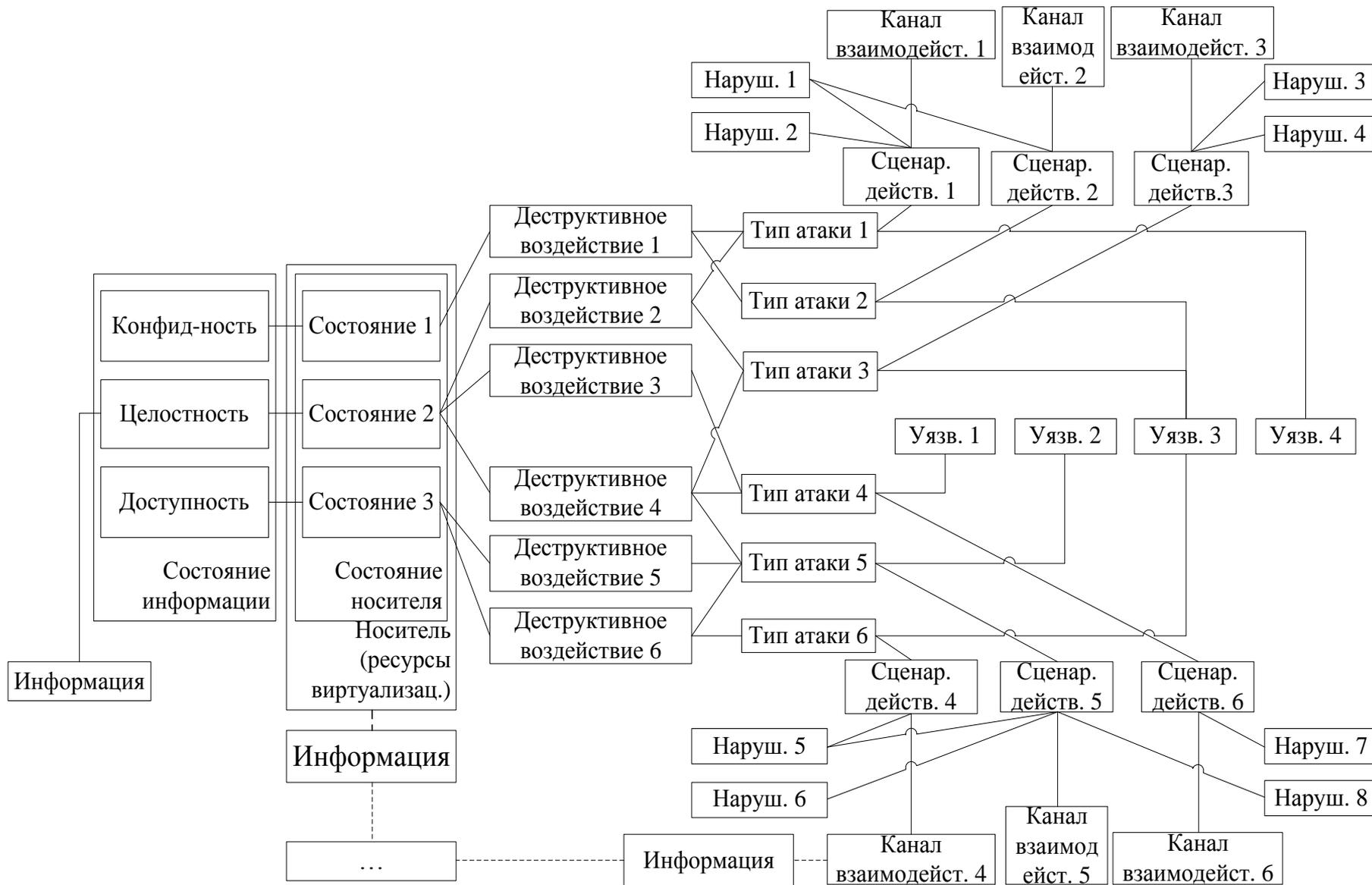
Ментальная карта понятия угроза



Иерархия носителей информации



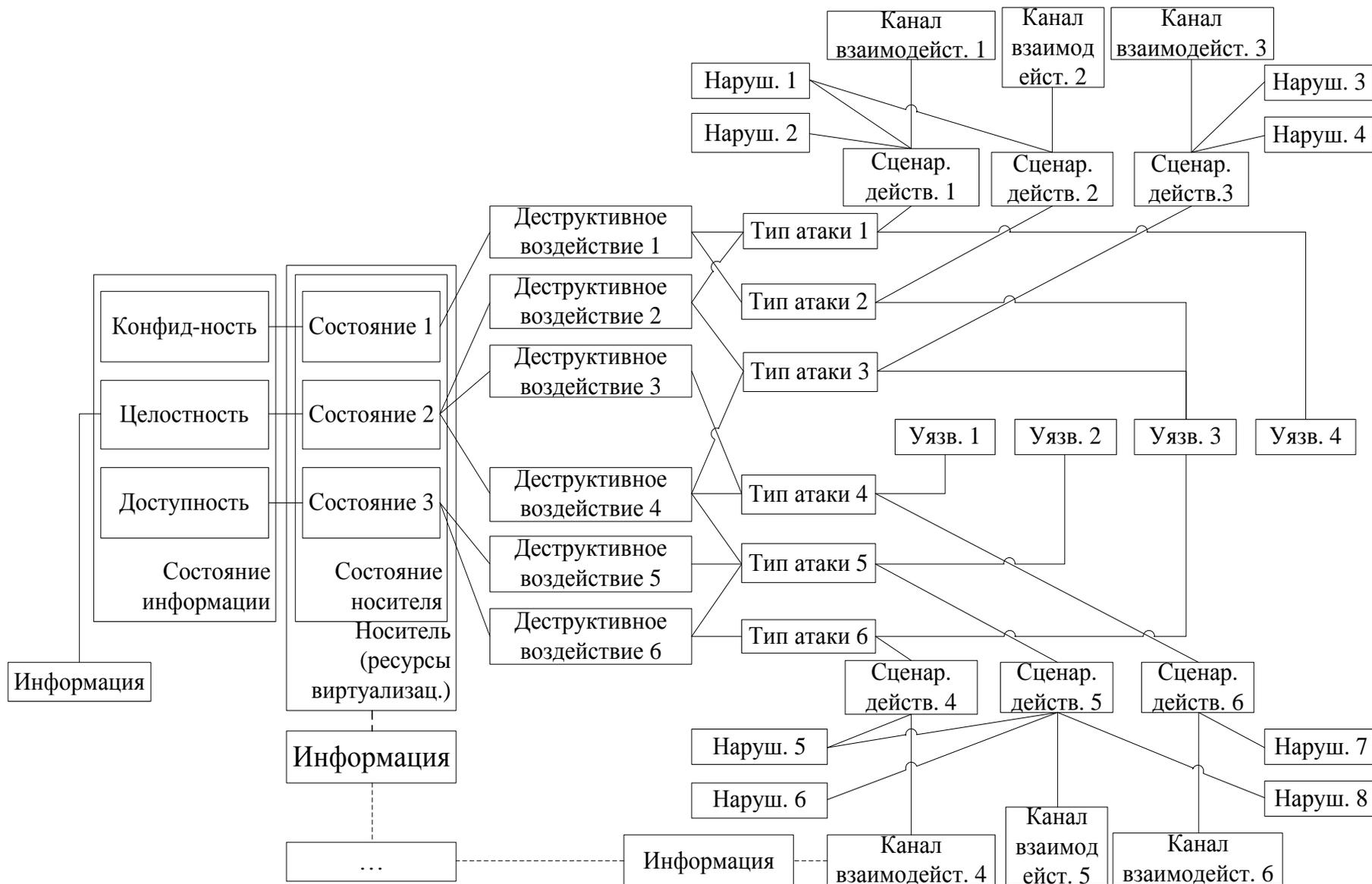
Ментальная карта понятия угроза



Состояние защищенности носителя

Состояние информации	Состояние физического носителя	Состояние логического носителя
Конфиденциальность информации	Доступность чтения только разрешенными интерфейсами	Доступность чтения носителя только для легитимных функций, запущенных легитимным пользователем
Целостность информации	Доступность записи только разрешенными интерфейсами	Доступность записи на носитель только для легитимных функций, запущенных легитимным пользователем
Доступность информации	Наличие функционирующего физического канала связи с пользователем информации	Наличие функционирующего логического канала связи информации с пользователем информации

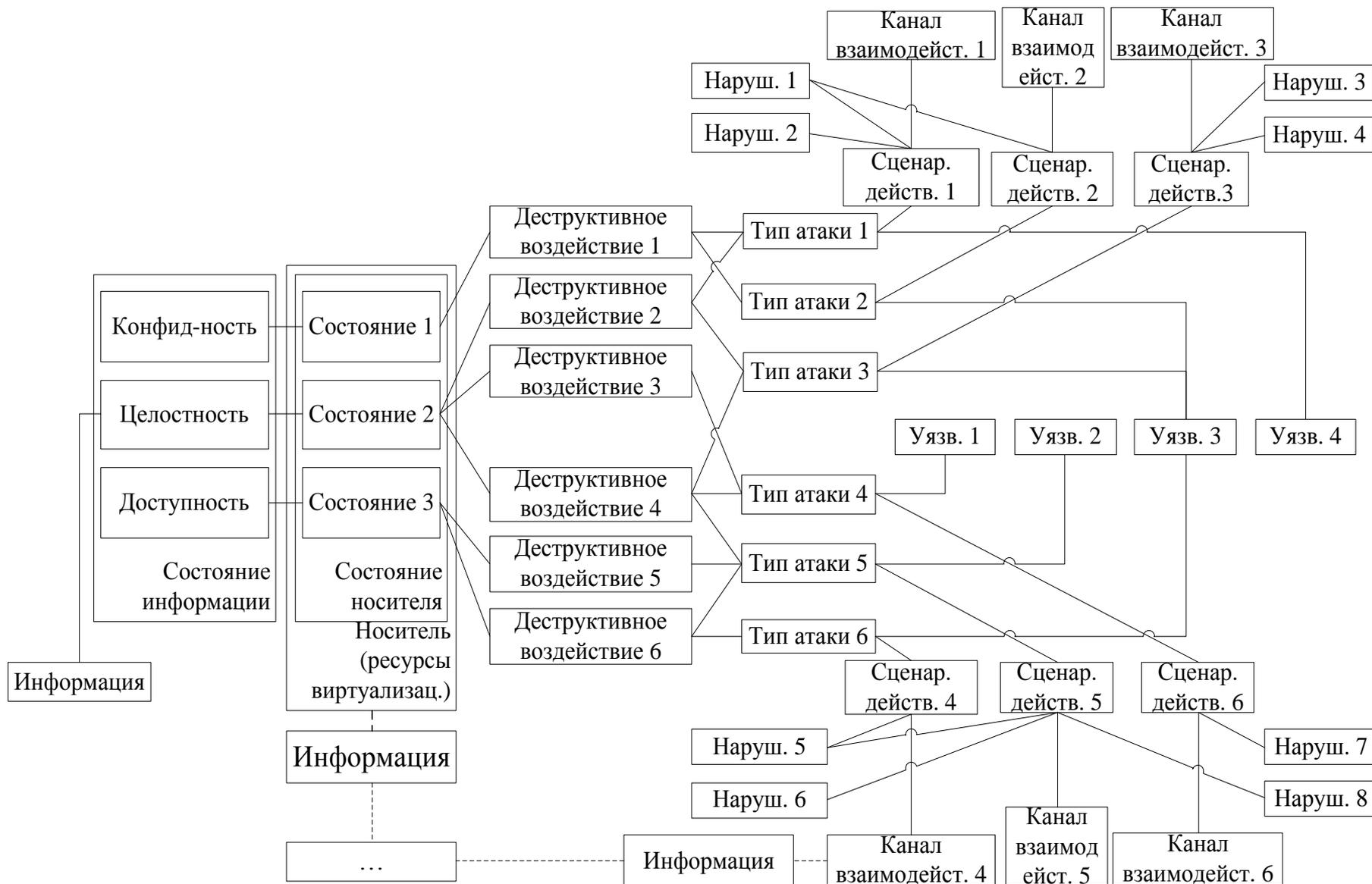
Ментальная карта понятия угроза



Типы воздействий, меняющие состояние носителей

Состояние носителя	Деструктивное воздействие
Доступность чтения только разрешенными интерфейсами	Подключение носителя к нелегитимному интерфейсу, через который можно получить с носителя ту же информацию, что и при подключении через легитимный.
Доступность записи только разрешенными интерфейсами	Подключение носителя к нелегитимному интерфейсу, через который можно записать на носитель ту же информацию, что и при подключении через легитимный.
Наличие функционирующего физического канала связи с пользователем информации	Физическое отключение носителя от инфраструктуры.
	Физическое повреждение носителя.
	Повреждение логической структуры носителя.
	Исчерпания вычислительной мощности обмена данных с физическим носителем.

Ментальная карта понятия угроза



Базы уязвимостей

Sponsored by DHS/NCCIC/US-CERT

NIST National Institute of Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities	Checklists	800-53/800-53A	Product Dictionary	Impact Metrics	Data Feeds	Statistics	FAQs
Home	SCAP	SCAP Validated Tools	SCAP Events	About	Contact	Vendor Comments	Visualizations

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains: 75506 CVE Vulnerabilities

Search Results (Refine Search)

There are 1 matching records.

Search Parameters:

- Keyword (text search): CVE-2012-1666
- Search Type: Search All
- Contains Software Flaws (CVE)

CVE-2012-1666

Summary: Untrusted search path vulnerability in VMware Tools in VMware Workstation before 8.0.4, VMware Player before 4.0.4, VMware Fusion before 4.1.2, VMware View before 5.1, and VMware ESX 4.1 before U3 and 5.0 before P03 allows local users to gain privileges via a Trojan horse tpfc.dll file in the current working directory.

Published: 9/8/2012 6:28:20 AM

CVSS Severity: v2 - 6.9 MEDIUM

TOTAL CVE-IDs: 74670

HOME > CVE > CVE-2015-6932

About CVE

FAQs

CVE List

Search & Downloads

Updates & Feeds

Coverage Goals

Request a CVE-ID

CVE Numbering Authorities (CNAs)

CVE In Use

Scoring (via NVD)

Fix Info (via NVD)

CVE-Compatible Products

News

Free Newsletter

Community

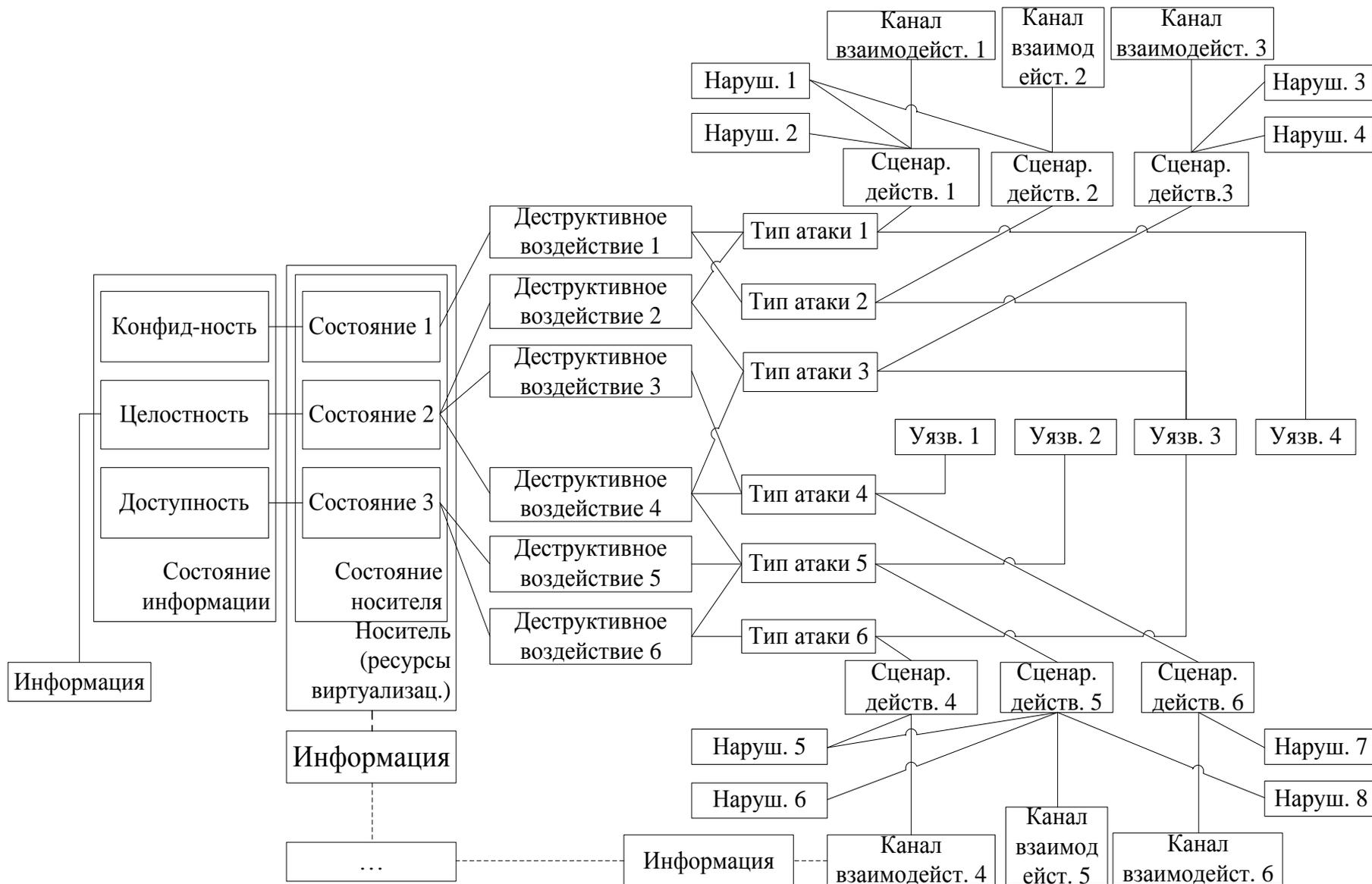
CVE Editorial Board

Board Discussion Archives

[Printer-Friendly View](#)

CVE-ID	
CVE-2015-6932	Learn more at National Vulnerability Database (NVD) <ul style="list-style-type: none">Severity RatingFix InformationVulnerable Software VersionsSCAP Mappings
Description	
VMware vCenter Server 5.5 before u3 and 6.0 before u1 does not verify X.509 certificates from TLS LDAP servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
<ul style="list-style-type: none">CONFIRM:http://www.vmware.com/security/advisories/VMSA-2015-0006.html	
Date Entry Created	
20150914	Disclaimer: The entry creation date may reflect when the CVE-ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Ментальная карта понятия угроза



Заключение

Разработанная модель идентификации угроз находится в стадии апробации как основа для структуры данных в информационной системе для автоматизированного формирования, анализа и актуализации модели угроз безопасности виртуальной инфраструктуры.