НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ ЭКОНОМИКИ И УПРАВЛЕНИЯ «НИНХ»

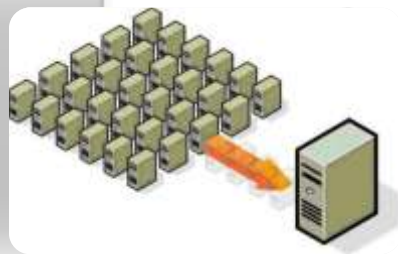
Кафедра информационной безопасности

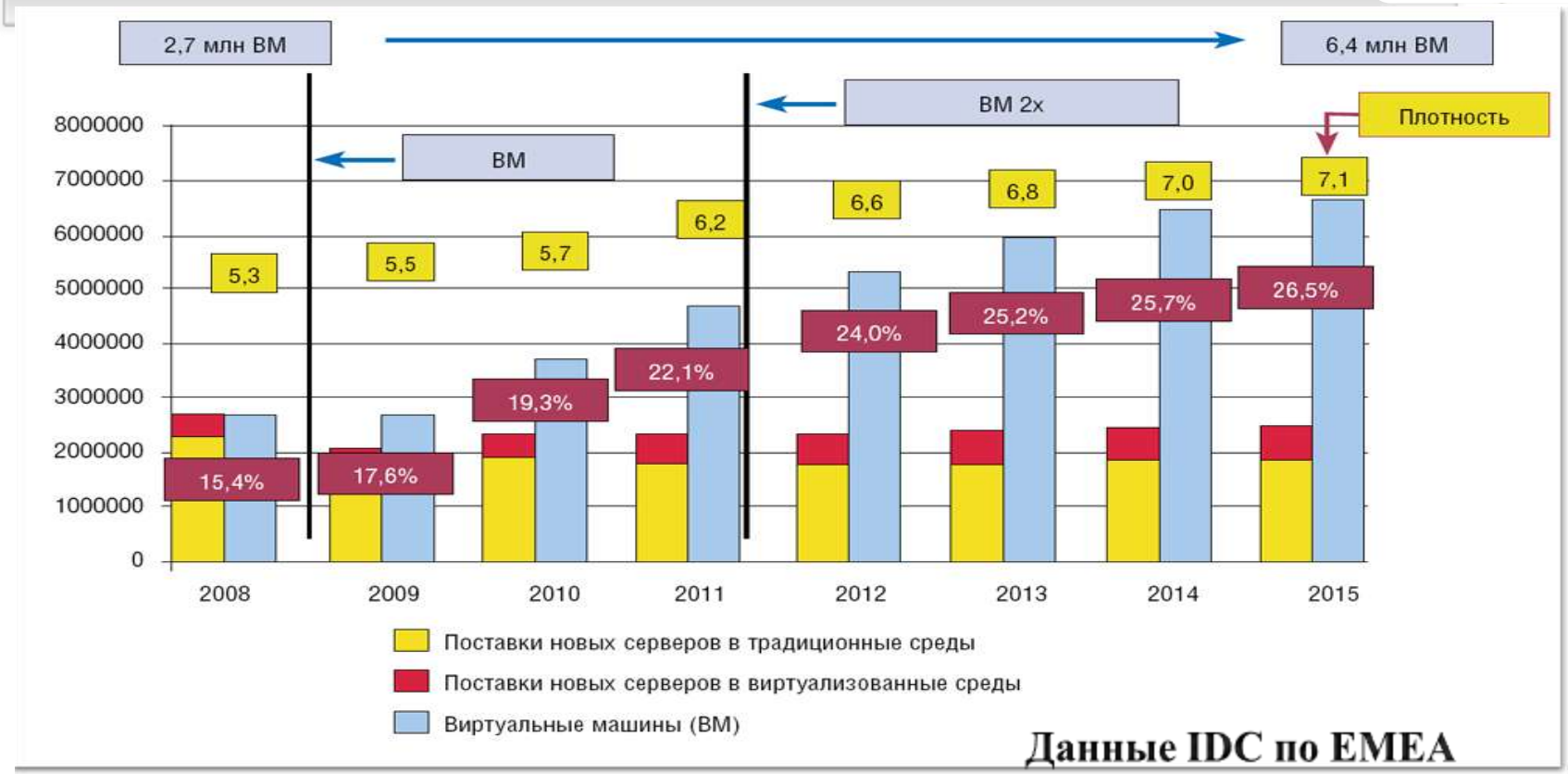
Модель идентификации угроз виртуальной инфраструктуры

Курносов 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.





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

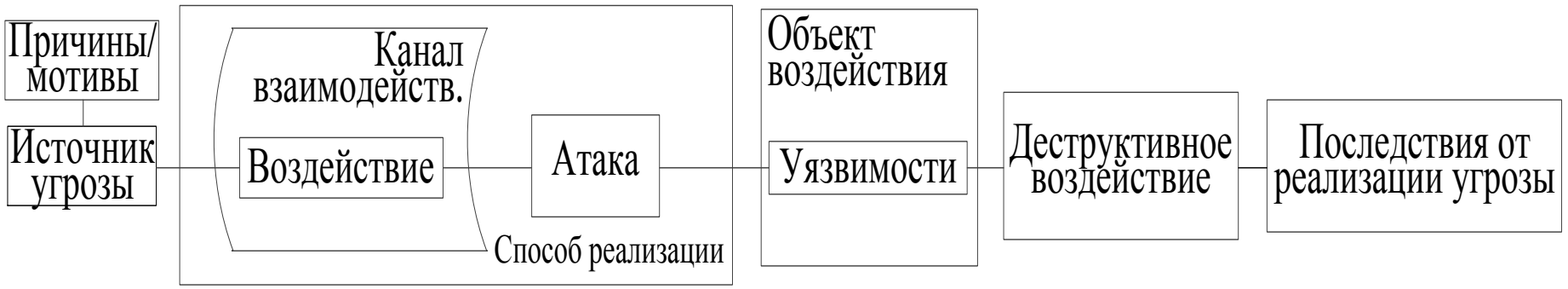
Задача идентификации угроз

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.

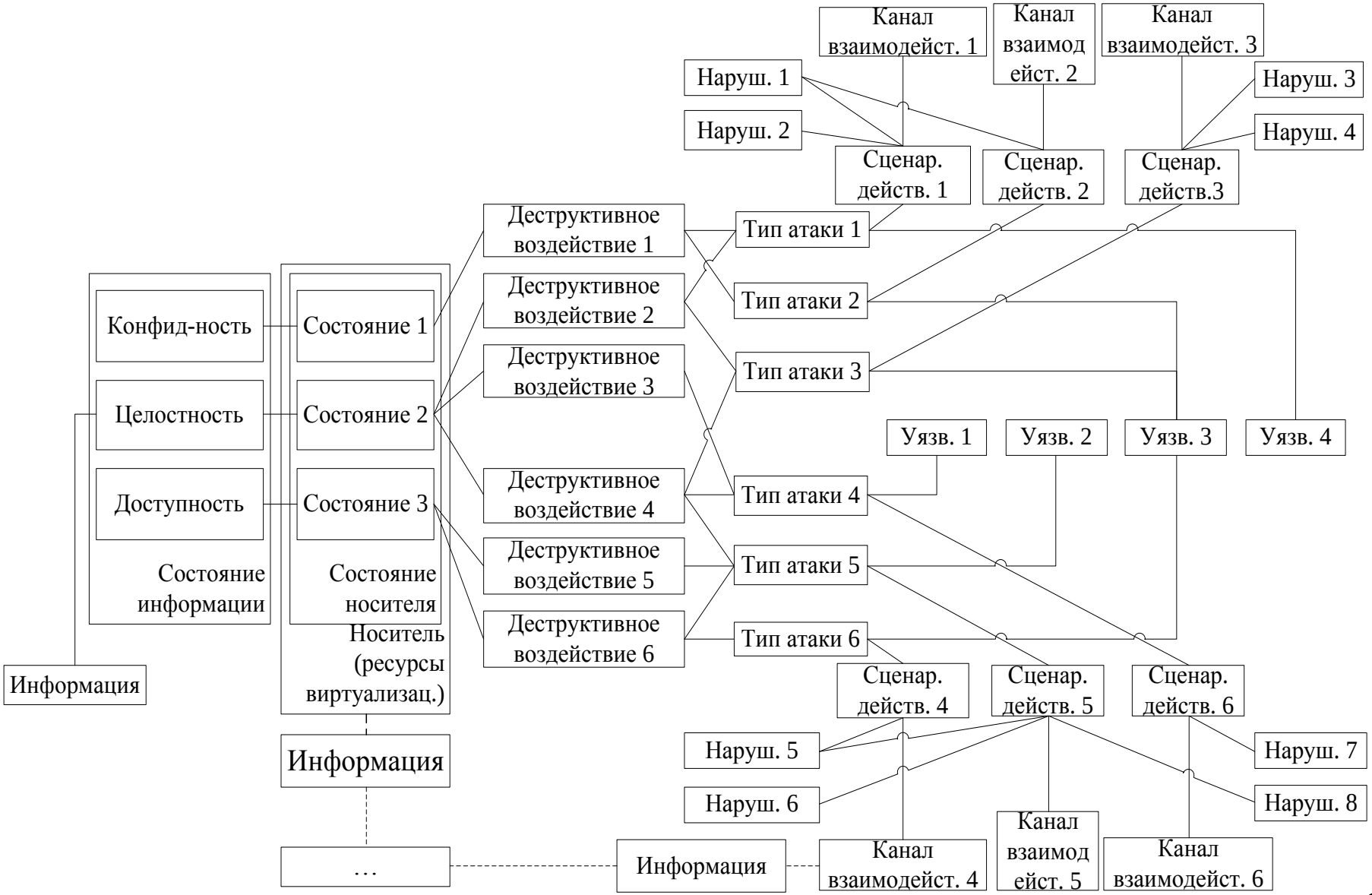
Задача идентификации угроз



Атрибуты идентифицированной угрозы:

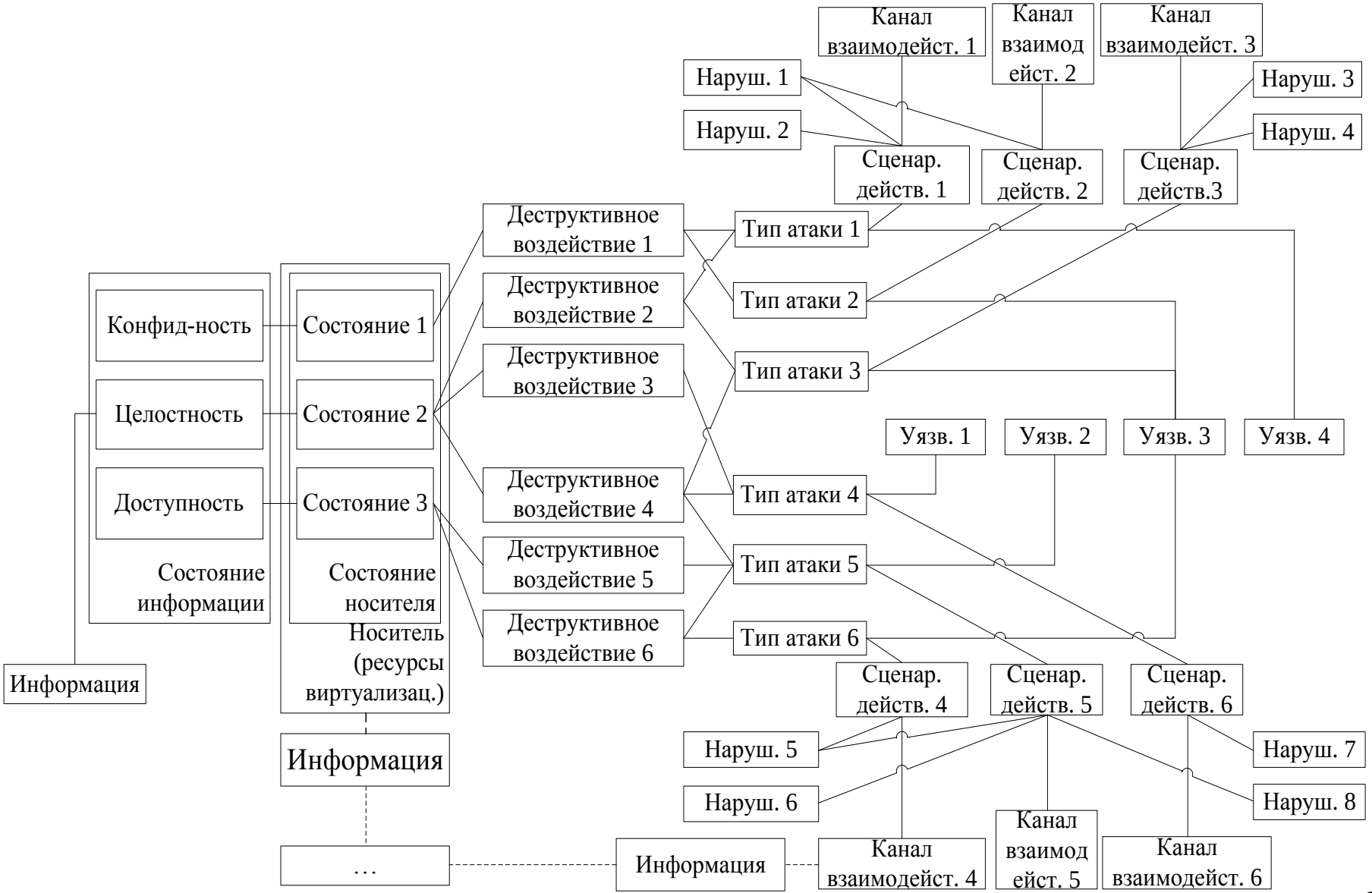
- источник угрозы (нарушитель);
- уязвимость;
- способ реализации;
- объект воздействия;
- последствия.

Ментальная карта понятия угроза



Иерархия носителей информации

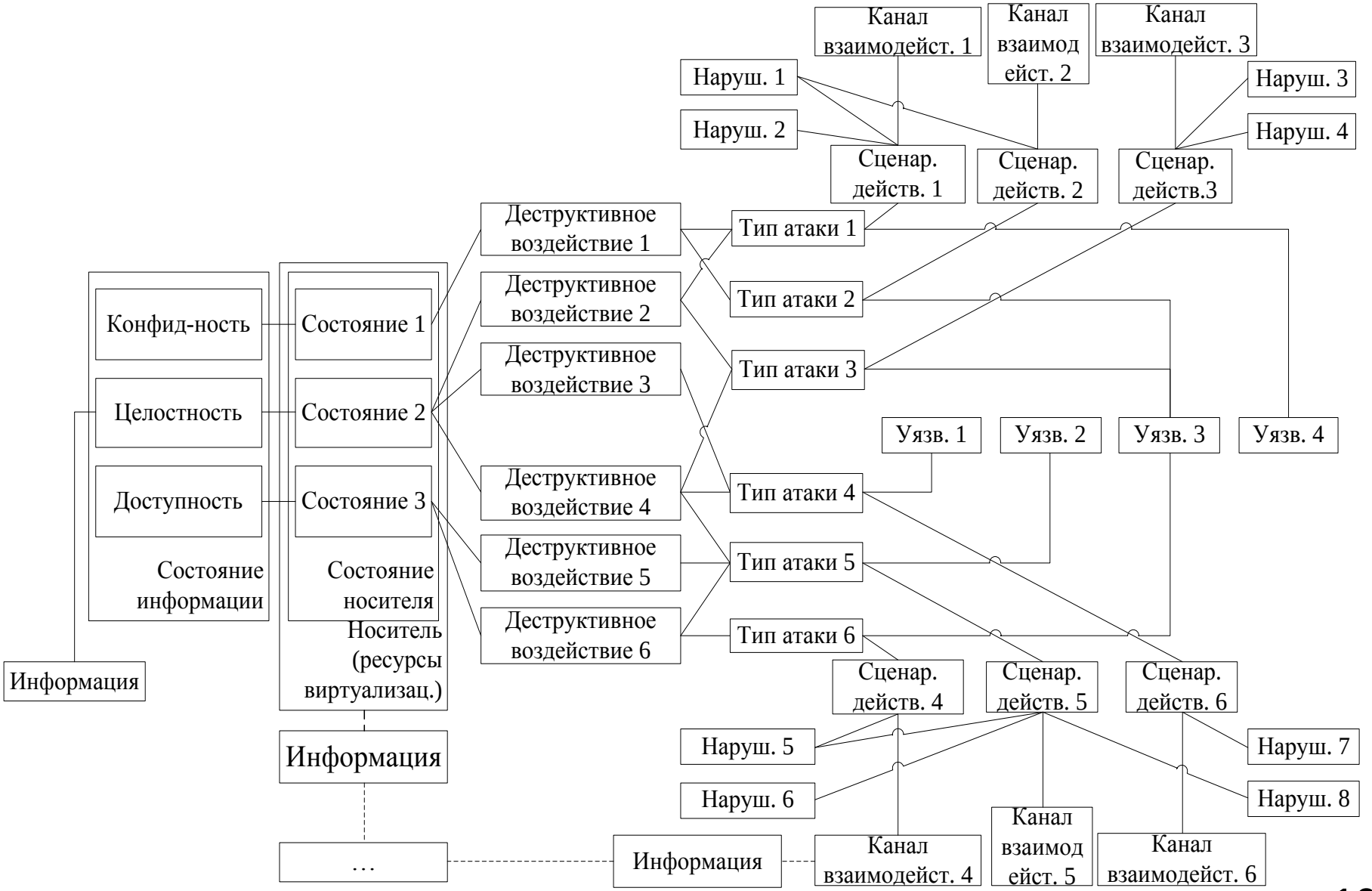
Ментальная карта понятия угроза



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

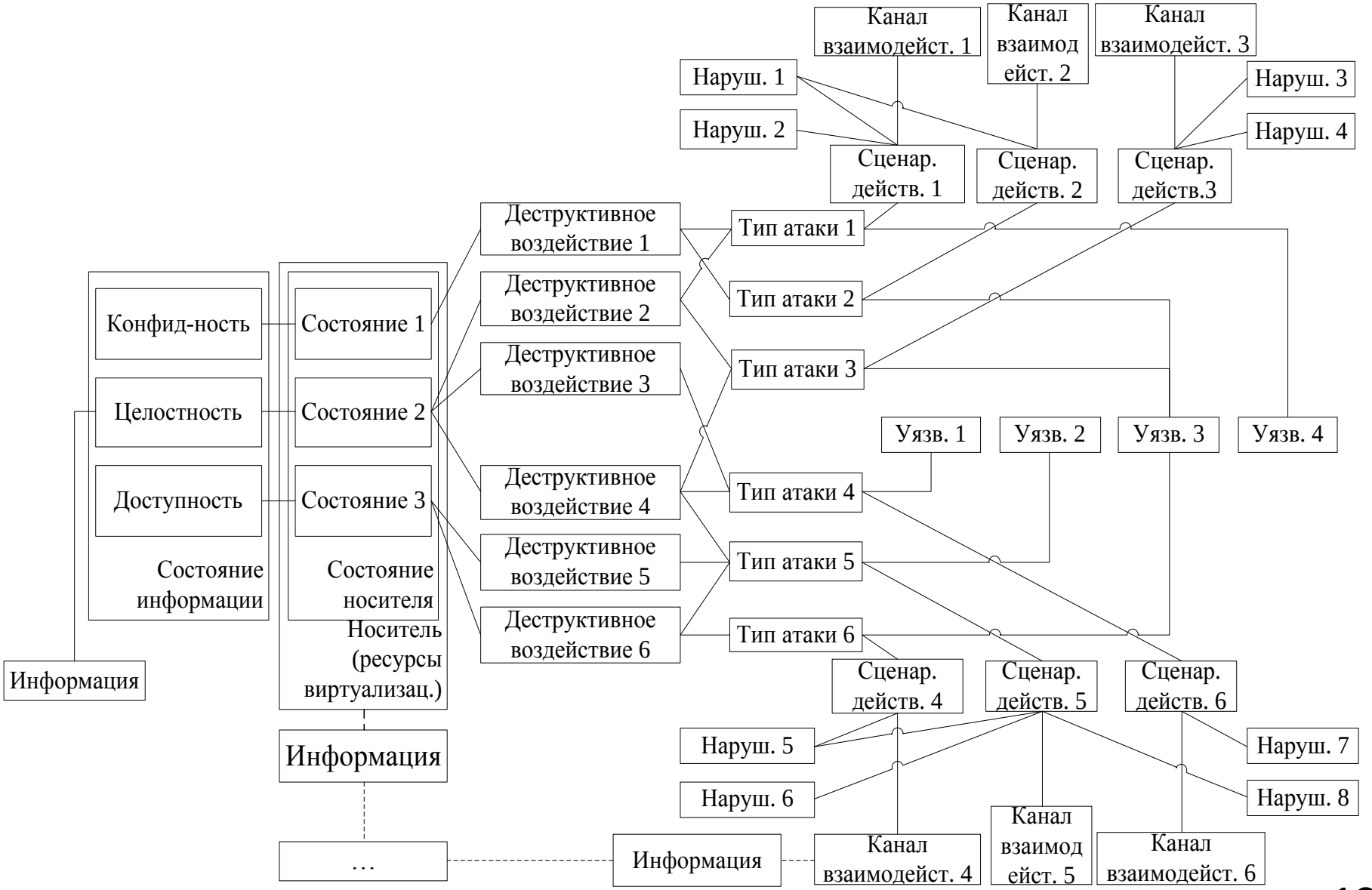
Ментальная карта понятия угроза



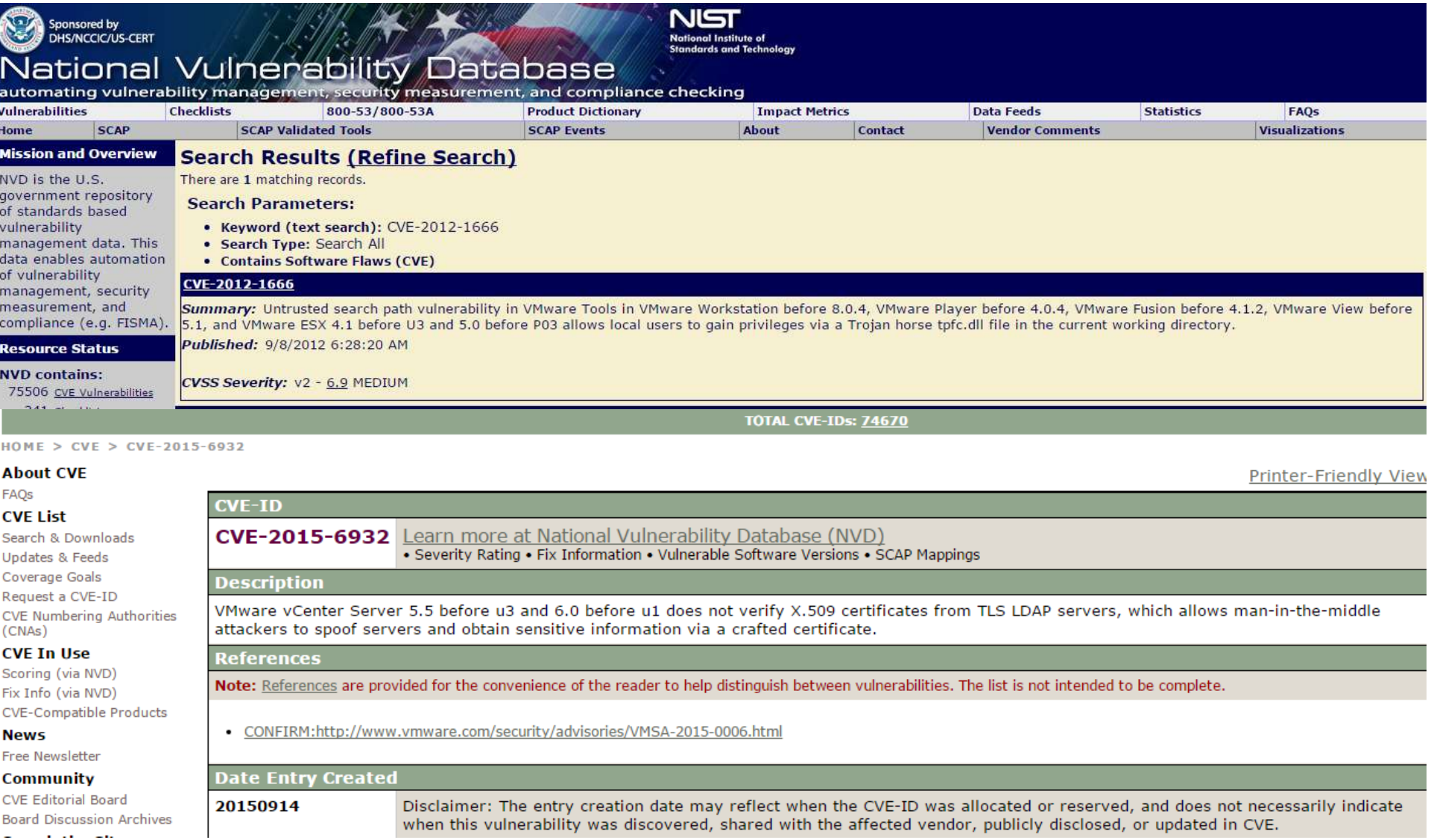
Типы воздействий, меняющие состояние носителей

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.

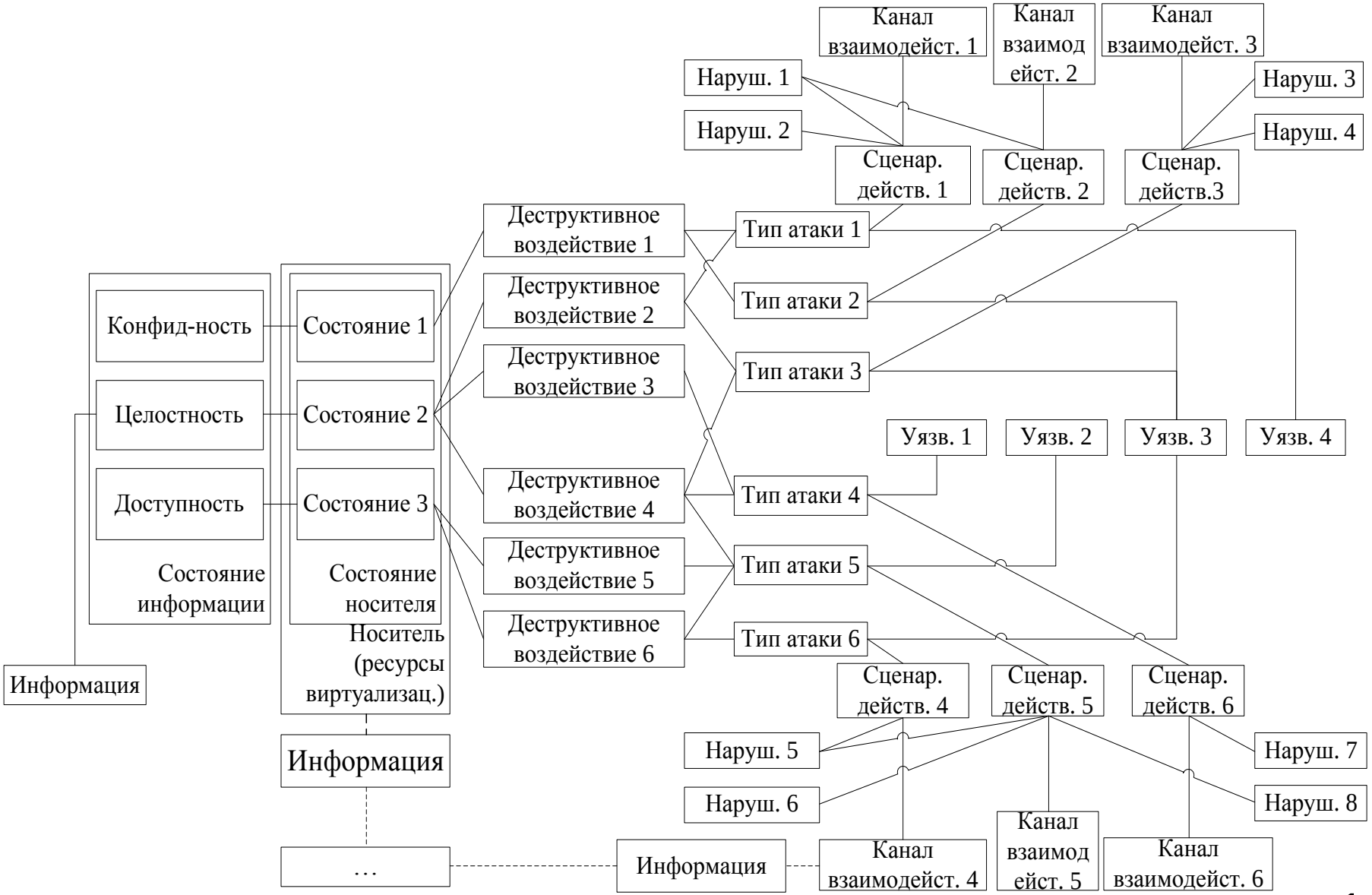
Ментальная карта понятия угроза



Базы уязвимостей



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.