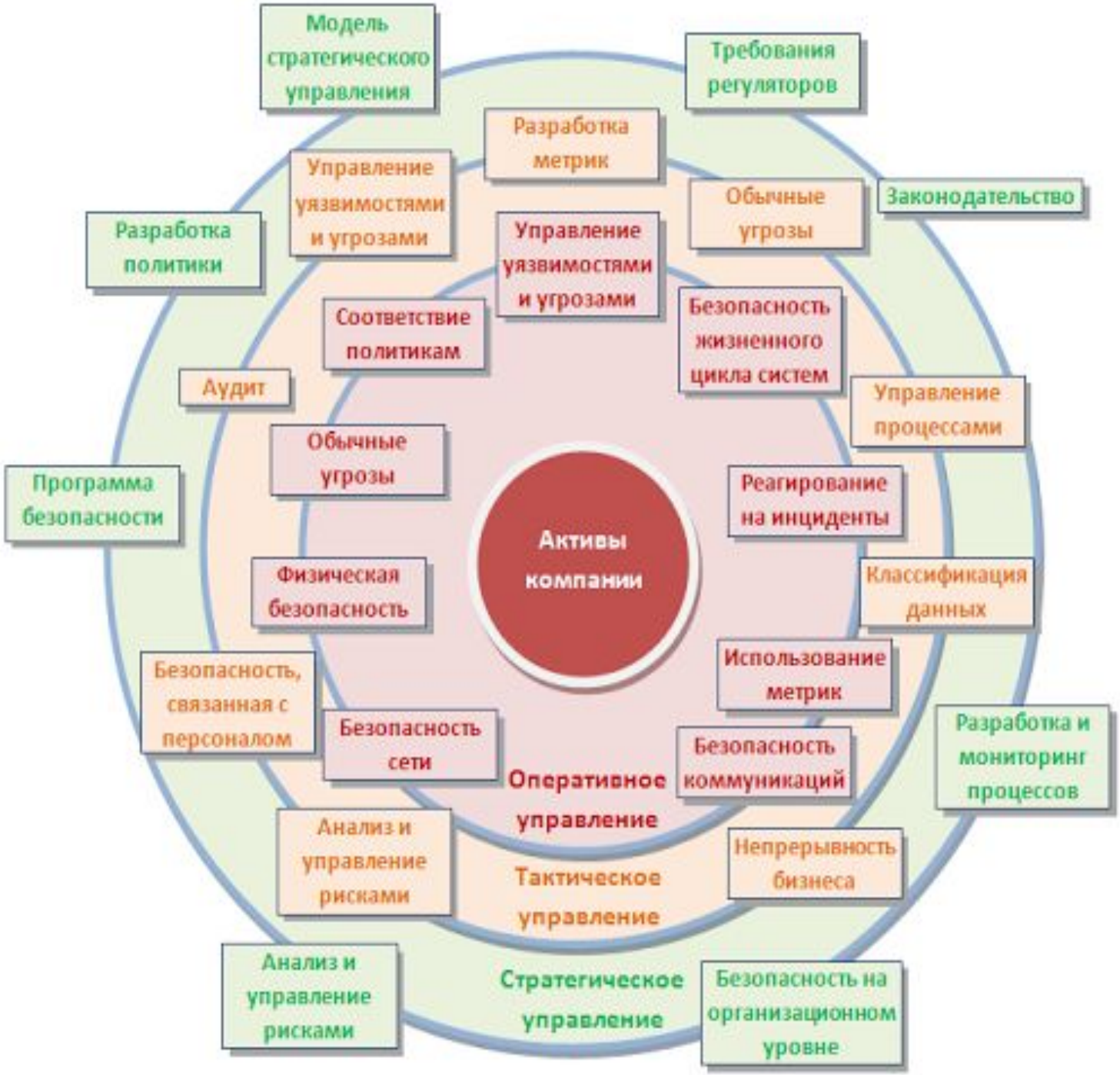
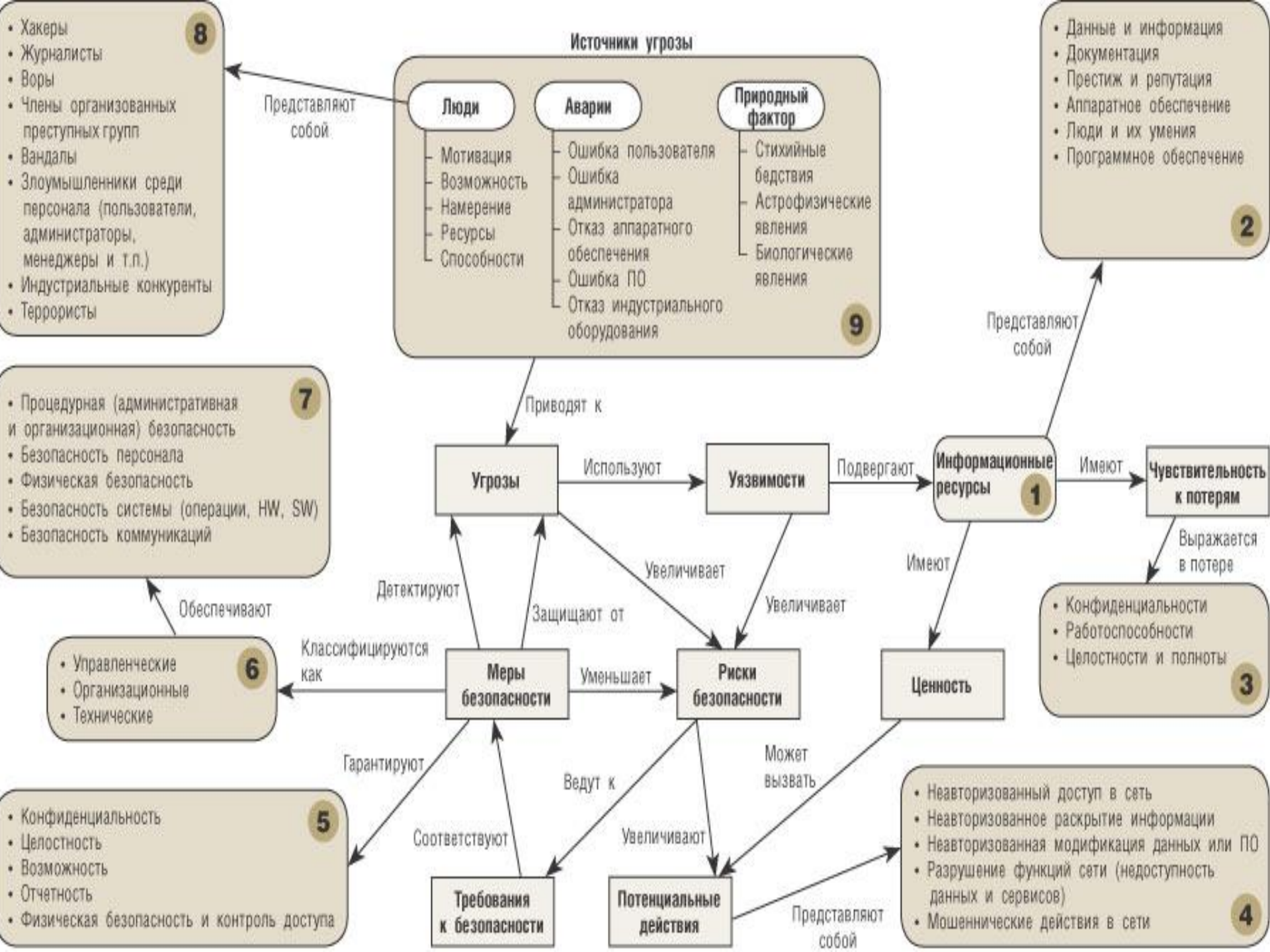
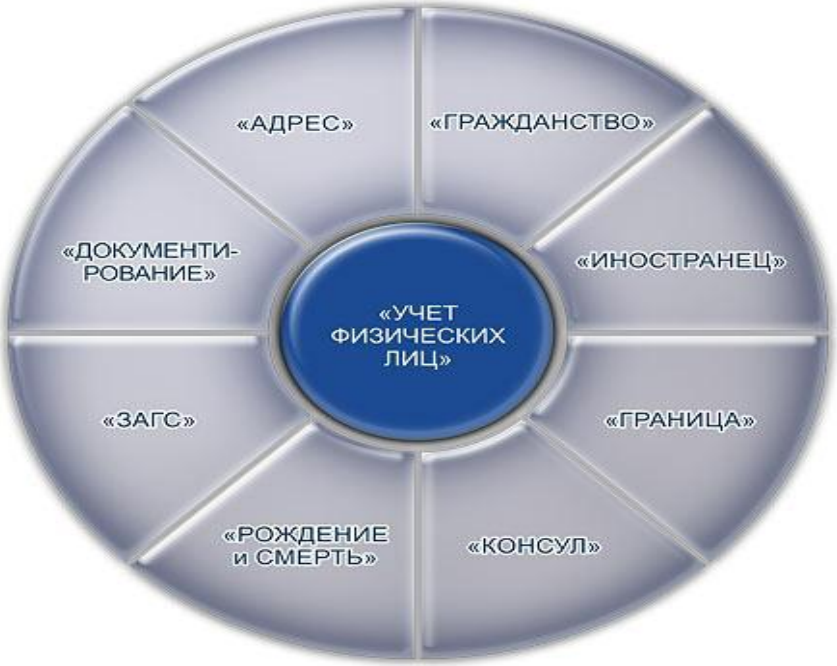
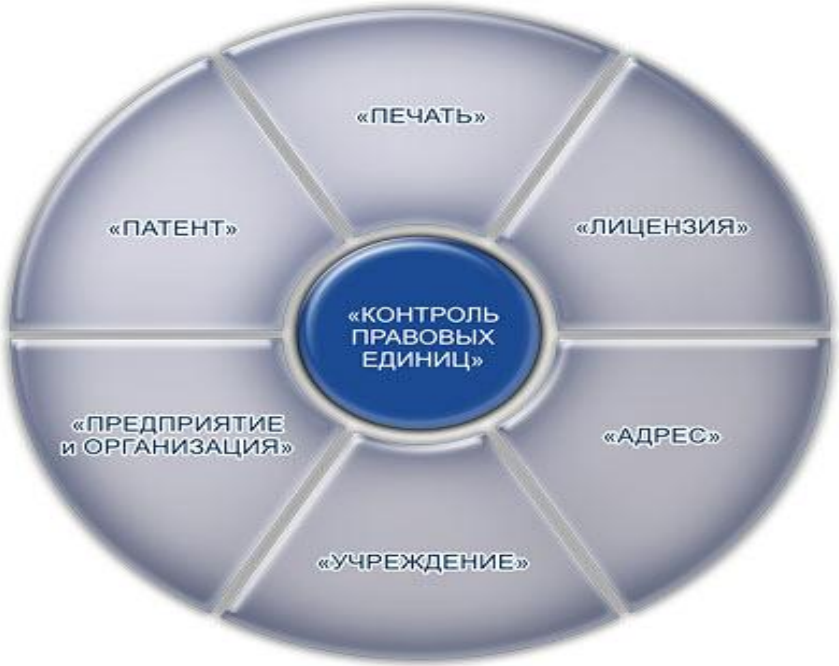

Модель стратегического управления
Требования регуляторов
Разработка метрик
Управление уязвимостями и угрозами
Обычные угрозы
Законодательство
Разработка политики
Управление уязвимостями и угрозами
Безопасность жизненного цикла систем
Соответствие политикам
Аудит
Управление процессами
Обычные угрозы
Программа безопасности
Реагирование на инциденты
Активы компании
Физическая безопасность
Классификация данных
Использование метрик
Безопасность, связанная с персоналом
Безопасность сети
Безопасность коммуникаций
Разработка и мониторинг процессов
Оперативное управление
Анализ и управление рисками
Непрерывность бизнеса
Тактическое управление
Анализ и управление рисками
Стратегическое управление
Безопасность на организационном уровне


Источники угрозы
Люди
Мотивация
Возможность
Намерение
Ресурсы
Способности
Аварии
Ошибка пользователя
Ошибка администратора
Отказ аппаратного обеспечения
Ошибка ПО
Отказ индустриального оборудования
Природный фактор
Стихийные бедствия
Астрофизические явления
Биологические явления
9
Представляют собой
Хакеры
Журналисты
Воры
Члены организованных преступных групп
Вандалы
Злоумышленники среди персонала (пользователи, администраторы, менеджеры и т.п.)
Индустриальные конкуренты
Террористы
8
Данные и информация
Документация
Престиж и репутация
Аппаратное обеспечение
Люди и их умения
Программное обеспечение
2
Представляют собой
Приводят к
Процедурная (административная и организационная) безопасность
Безопасность персонала
Физическая безопасность
Безопасность системы (операции, HW, SW)
Безопасность коммуникаций
7
Обеспечивают
Угрозы
Используют
Уязвимости
Подвергают
Информационные ресурсы
1
Имеют
Чувствительность к потерям
Выражается в потере
Конфиденциальности
Работоспособности
Целостности и полноты
3
Детектируют
Защищают от
Увеличивает
Увеличивает
Имеют
Управленческие
Организационные
Технические
6
Классифицируются как
Меры безопасности
Уменьшает
Риски безопасности
Ценность
Гарантируют
Ведут к
Может вызвать
Конфиденциальность
Целостность
Возможность
Отчетность
Физическая безопасность и контроль доступа
5
Соответствуют
Увеличивают
Требования к безопасности
Потенциальные действия
Представляют собой
Неавторизованный доступ в сеть
Неавторизованное раскрытие информации
Неавторизованная модификация данных или ПО
Разрушение функций сети (недоступность данных и сервисов)
Мошеннические действия в сети
4


«УЧЕТ ФИЗИЧЕСКИХ ЛИЦ»
«АДРЕС»
«ГРАЖДАНСТВО»
«ИНОСТРАНЕЦ»
«ГРАНИЦА»
«КОНСУЛ»
«РОЖДЕНИЕ и СМЕРТЬ»
«ЗАГС»
«ДОКУМЕНТИ-РОВАНИЕ»


«КОНТРОЛЬ ПРАВОВЫХ ЕДИНИЦ»
«ПЕЧАТЬ»
«ЛИЦЕНЗИЯ»
«АДРЕС»
«УЧРЕЖДЕНИЕ»
«ПРЕДПРИЯТИЕ и ОРГАНИЗАЦИЯ»
«ПАТЕНТ»


УЧЕТ ТРАНСПОРТА
АВТОМОБИЛЬ
АГРЕГАТ
ТЕСТИРОВАНИЕ
СОБСТВЕННОСТЬ
ДОКУМЕНТИРОВАНИЕ
РЕГИСТРАЦИОННЫЙ ЗНАК


«УЧЕТ ВОДИТЕЛЕЙ»
«ЭКЗАМЕН»
«МЕДИЦИНСКИЕ ПОКАЗАНИЯ»
«ПРАВО УПРАВЛЕНИЯ»
«ДОКУМЕНТИ-РОВАНИЕ»
«УЧЕБНОЕ УЧРЕЖДЕНИЕ»
«ПРАВО-НАРУШЕНИЕ»
«ПОДГОТОВКА и ПЕРЕ-ПОДГОТОВКА»

ресурсов недвижимости
агротехнических ресурсов
лесных ресурсов
водных ресурсов
градостроительных ресурсов
экологических ресурсов
геологических ресурсов
культурно-исторических ресурсов
промышленных ресурсов
чрезвычайных ситуаций и опасных природных явлений
специальные

ТЕМАТИЧЕСКИЕ ЭЛЕКТРОННЫЕ КАРТЫ
(автоматизированный учет природных ресурсов
и техногенного потенциала)

БАЗОВАЯ ПРОСТРАНСТВЕННАЯ
МОДЕЛЬ МЕСТНОСТИ

кадастровые планы

административно-территориальное устройство
и адресные планы населенных пунктов

базовая электронная карта

Содержание разрядов:

1	Г Г Г	Х Х Х	Y Y Y Y Y	К

1 - признак идентификационного номера - номер главного раздела, к которому относится объект идентификации

Г Г Г - три последние цифры года присвоения IDNO

Х Х Х - код органа, зарегистрировавшего правовую единицу

Y Y Y Y Y - порядковый номер регистрации, в соответствующем году в данном офисе

К - контрольная цифра

Пример:

1	2 9 5	8 7 3	3 2 1 5 8	9

Содержание разрядов:

2	Г Г Г	Х Х Х	Y Y Y Y Y	К

2 - признак идентификатора физического лица во множестве государственных идентификаторов

Г Г Г - три последние цифры года присвоения IDNP

Х Х Х - код офиса регистратора

Y Y Y Y Y - порядковый номер записи в соответствующем году в данном офисе

К - контрольная цифра

Пример:

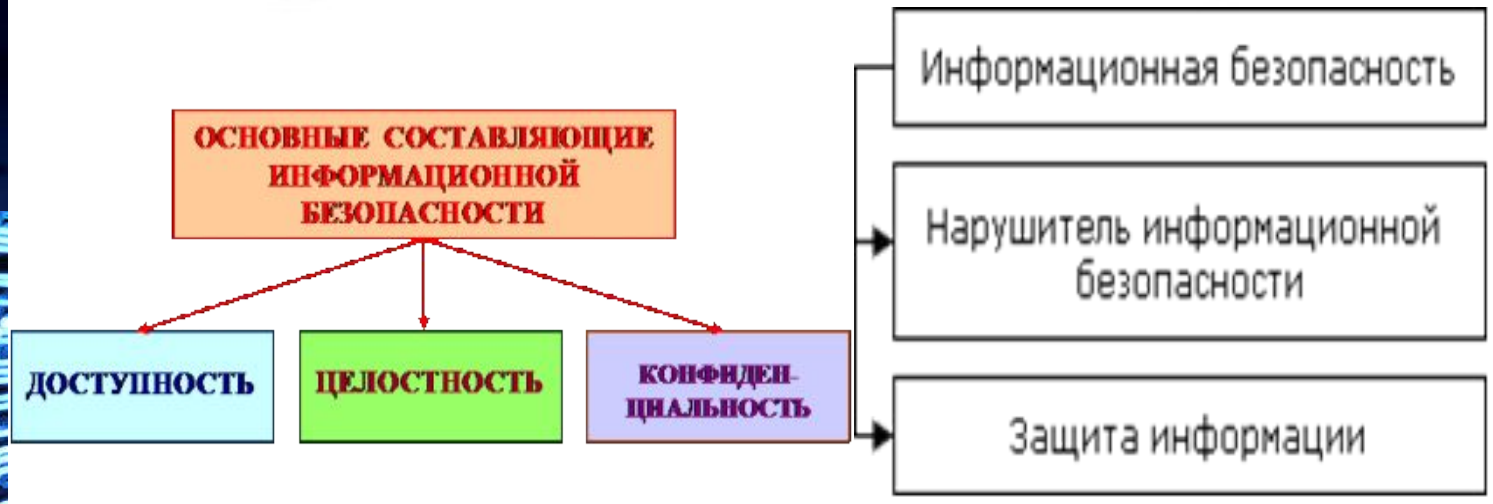
2	0 0 9	0 8 8	0 0 1 5 6	9


Данные
Информация
Системы
Коммуникации
Технологии
Регламентация
Контроль и
регистрация
Субъект
легального
доступа
Субъекты нелегального доступа
Вредоносные программы
Что
защищать?
От кого
защищать?
Как и чем защищать?

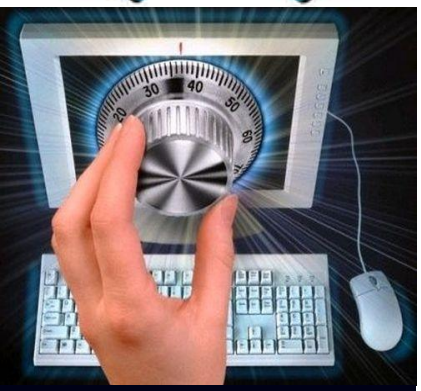
"ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ - это состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государств" (Закон РФ "Об участии в международном информационном обмене")

- Информация - это всеобщее свойство материи.
- Любое взаимодействие в природе и обществе основано на информации.
- Всякий процесс совершения работы есть процесс информационного взаимодействия.
- Информация - продукт отражения действительности.
- Действительность отражается в пространстве и времени.
- Ничего не происходит из ничего.
- Информация сохраняет свое значение в неизменном виде доя тех пор, пока остается в неизменном виде носитель информации - ПАМЯТЬ.
- Ничто не исчезает просто так.


Доступ-
ность
Цели
безопас
ности
Целост-
ность
Конфи-
денциа
льность


ОСНОВНЫЕ СОСТАВЛЯЮЩИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ДОСТУПНОСТЬ
ЦЕЛОСТНОСТЬ
КОНФИДЕН-
ЦИАЛЬНОСТЬ
Информационная безопасность
Нарушитель информационной безопасности
Защита информации

Составляющие информационной безопасности



Доступность – это гарантия получения требуемой информации или информационной услуги пользователем за определенное время.

Целостность – гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений. Целостность информации условно подразделяется на статическую и динамическую.

Конфиденциальность – гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена.

Задачи информационной безопасности

В этой связи основными задачами информационной безопасности в широком смысле являются:

- защита государственной тайны, т. е. секретной и другой конфиденциальной информации, являющейся собственностью государства, от всех видов несанкционированного доступа, манипулирования и уничтожения;
- защита прав граждан на владение, распоряжение и управление принадлежащей им информацией;
- защита прав предпринимателей при осуществлении ими коммерческой деятельности;
- защита конституционных прав граждан на тайну переписки, переговоров, личную тайну.

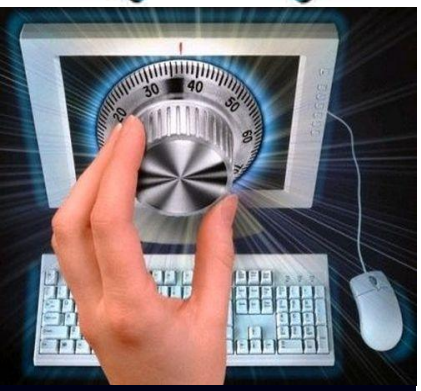
Рассматривая проблему информационной безопасности в узком смысле

- защита технических и программных средств информатизации от ошибочных действий персонала и техногенных воздействий, а также стихийных бедствий;
- защита технических и программных средств информатизации от преднамеренных воздействий.

Задачи информационной безопасности

С учетом изложенного выделим три уровня формирования режима информационной безопасности:

- законодательно-правовой;
- административный (организационный);
- программно-технический.



Законодательно-правовой уровень включает комплекс законодательных и иных правовых актов, устанавливающих правовой статус субъектов информационных отношений, субъектов и объектов защиты, методы, формы и способы защиты, их правовой статус.

Административный уровень включает комплекс взаимокоординируемых мероприятий и технических мер, реализующих практические механизмы защиты в процессе создания и эксплуатации систем защиты информации.

Программно-технический уровень включает три подуровня: физический, технический (аппаратный) и программный.


НОРМАТИВНО-ПРАВОВАЯ ОСНОВА
КОНЦЕПЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Правовые документы
Организационно-распорядительные документы
Нормативные документы
Федеральные законы РФ
Кодексы РФ
Указы и Распоряжения Президента РФ
Постановления правительства РФ
Положения
Концепции
Руководства, инструкции
Распоряжения
ГОСТы
Международные стандарты
Руководящие документы
Специальные нормативные документы ФСТЭК (Гостехкомиссии) и ФСБ (ФАПСИ)
Документы, регламентирующие защиту информации от несанкционированного доступа
Документы, регламентирующие использование средств криптозащиты

1.Основополагающими документами по информационной безопасности в РФ являются Конституция РФ и Концепция национальной безопасности.

2.Законодательные меры в сфере информационной безопасности направлены на создание в стране законодательной базы, упорядочивающей и регламентирующей поведение субъектов и объектов информационных отношений, а также определяющей ответственность за нарушение установленных норм.

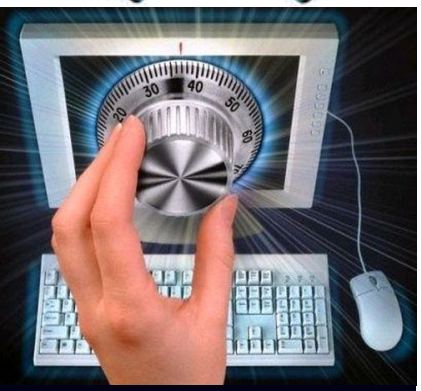
3.Закон РФ "Об информации, информатизации и защите информации" от 27 июля 2006 г. N 149-ФЗ является одним из основных базовых законов в области защиты информации, который регламентирует отношения, возникающие при формировании и использовании информационных ресурсов Российской Федерации на основе сбора, накопления, хранения, распространения и предоставления потребителям документированной информации, а также при создании и использовании информационных технологий, при защите информации и прав субъектов, участвующих в информационных процессах и информатизации.

4.Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

5.Система защиты государственной тайны – совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну и их носителей, а также мероприятий, проводимых в этих целях.

6.Немаловажная роль в системе правового регулирования информационных отношении отводится ответственности субъектов за нарушения в сфере информационной безопасности. Основными документами в этом направлении являются:

- Уголовный кодекс Российской Федерации;
- Кодекс Российской Федерации об административных правонарушениях



Модель нарушителя — (в информатике) абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа.

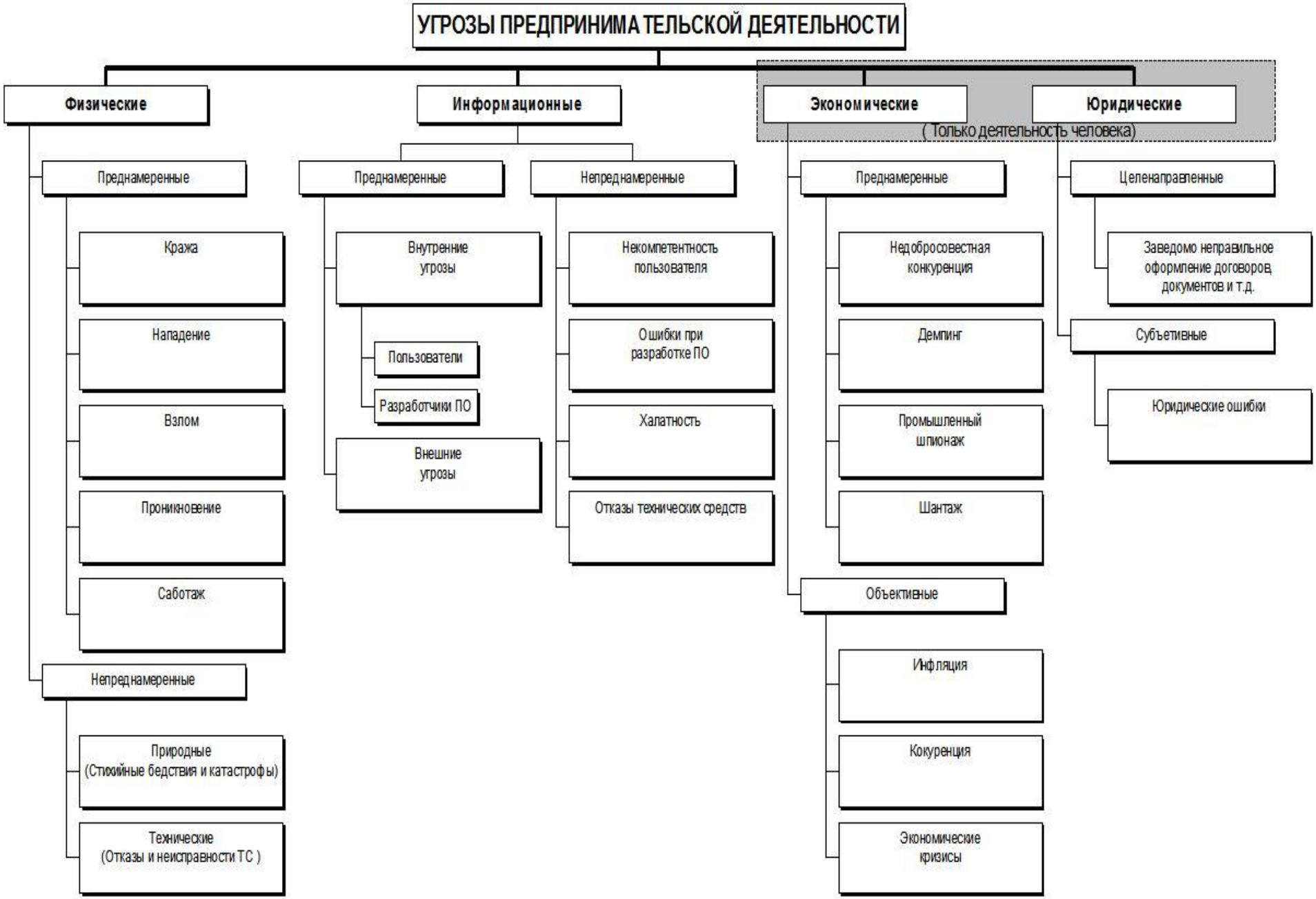
Модель нарушителя определяет:

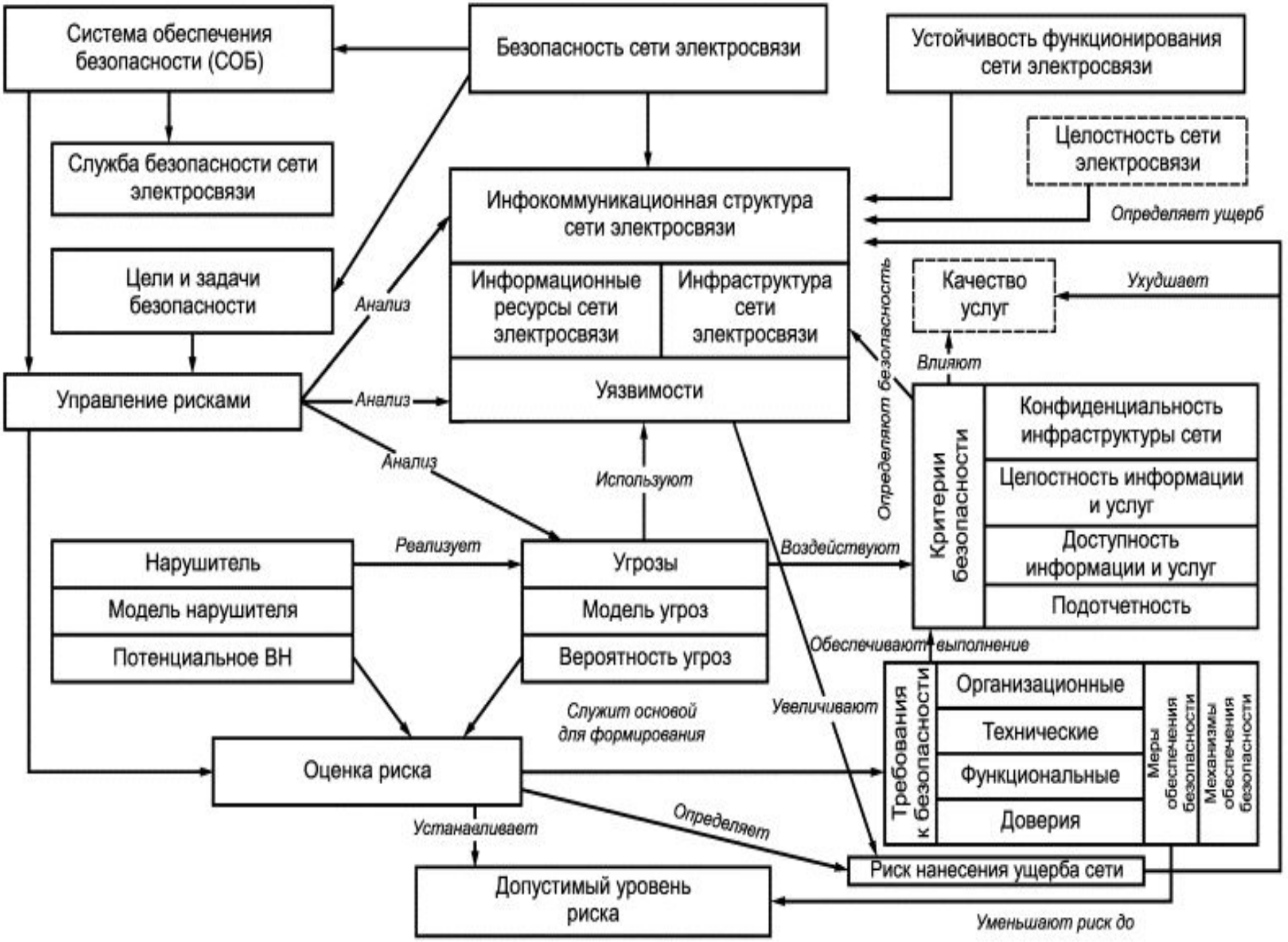
- категории (типы) нарушителей, которые могут воздействовать на объект; цели, которые могут преследовать нарушители каждой категории, возможный количественный состав, используемые инструменты, принадлежности, оснащение, оружие и проч.;
- типовые сценарии возможных действий нарушителей, описывающие последовательность (алгоритм) действий групп и отдельных нарушителей, способы их действий на каждом этап

Модель нарушителей может иметь разную степень детализации.

- Содержательная модель нарушителей отражает систему принятых руководством объекта, ведомства взглядов на контингент потенциальных нарушителей, причины и мотивацию их действий, преследуемые цели и общий характер действий в процессе подготовки и совершения акций воздействия.
- Сценарии воздействия нарушителей определяют классифицированные типы совершаемых нарушителями акций с конкретизацией алгоритмов и этапов, а также способов действия на каждом этапе.
- Математическая модель воздействия нарушителей представляет собой формализованное описание сценариев в виде логико-алгоритмической последовательности действий нарушителей, количественных значений, параметрически характеризующих результаты действий, и функциональных (аналитических, численных или алгоритмических) зависимостей, описывающих протекающие процессы взаимодействия нарушителей с элементами объекта и системы охраны. Именно этот вид модели используется для количественных оценок уязвимости объекта и эффективности охраны.

ОБОБЩЕННАЯ КЛАССИФИКАЦИЯ УГРОЗ




Система обеспечения безопасности (СОБ)
Безопасность сети электросвязи
Устойчивость функционирования сети электросвязи
Служба безопасности сети электросвязи
Целостность сети электросвязи
Определяет ущерб
Инфокоммуникационная структура сети электросвязи
Информационные ресурсы сети электросвязи
Инфраструктура сети электросвязи
Уязвимости
Цели и задачи безопасности
Анализ
Качество услуг
Ухудшает
Влияют
Определяют безопасность
Управление рисками
Анализ
Анализ
Используют
Критерии безопасности
Конфиденциальность инфраструктуры сети
Целостность информации и услуг
Доступность информации и услуг
Подотчетность
Нарушитель
Модель нарушителя
Потенциальное ВН
Реализует
Угрозы
Модель угроз
Вероятность угроз
Воздействуют
Обеспечивают выполнение
Требования к безопасности
Организационные
Технические
Функциональные
Доверия
Меры обеспечения безопасности
Механизмы обеспечения безопасности
Служит основой для формирования
Увеличивают
Оценка риска
Устанавливает
Определяет
Риск нанесения ущерба сети
Допустимый уровень риска
Уменьшают риск до