

Национальный исследовательский
университет
«Высшая школа экономики»

Институт проблем
безопасности

2015/2016-2016/2017 гг.

майнор



760 часов

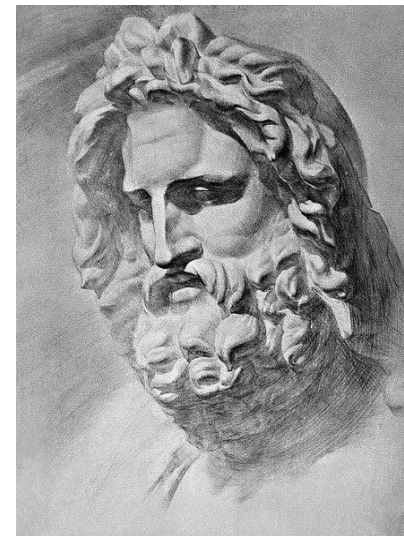


**Безопасность предпринимательской
деятельности**



Безопасность предпринимательской деятельности

3-й и 4-й модули 2016/2017 учебного года:
январь, февраль, март, апрель, май, июнь
190 академических часов



Дисциплина № 4

Организационное поведение в бизнесе и управление сложными системами безопасности

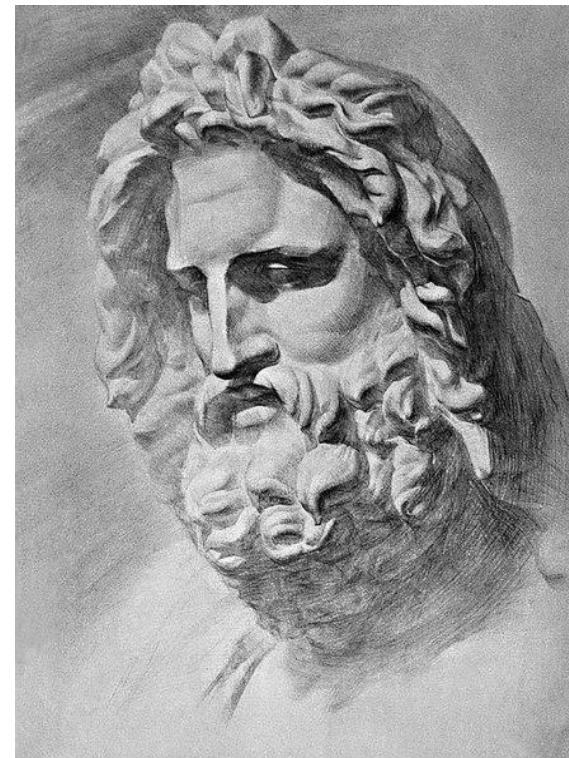


Организационное поведение в бизнесе и
управление сложными системами безопасности

Тема № 1

Понятие комплексной безопасности предприятия

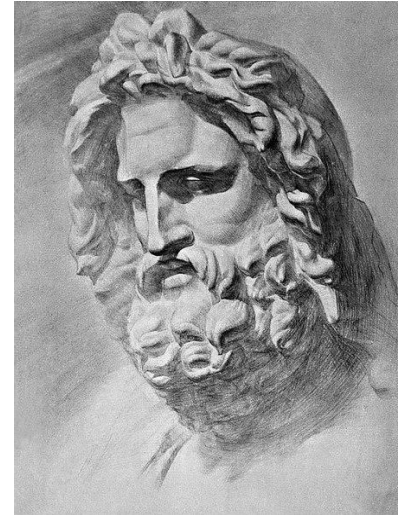
Лекция, 2 часа



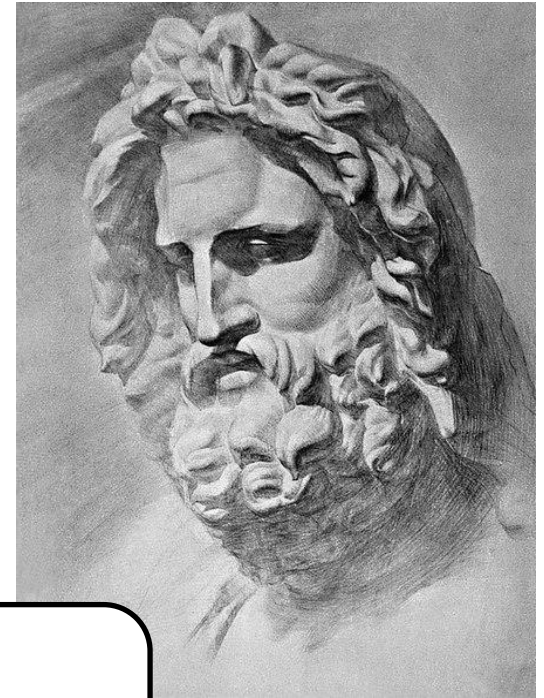
Зевс, Бог

Оглавление

1. Основные функции систем безопасности
2. Связанные функции и пограничные области деятельности
3. Универсальность системы безопасности в рамках предприятия
4. Принципы построения системы безопасности предприятия
5. Библиография



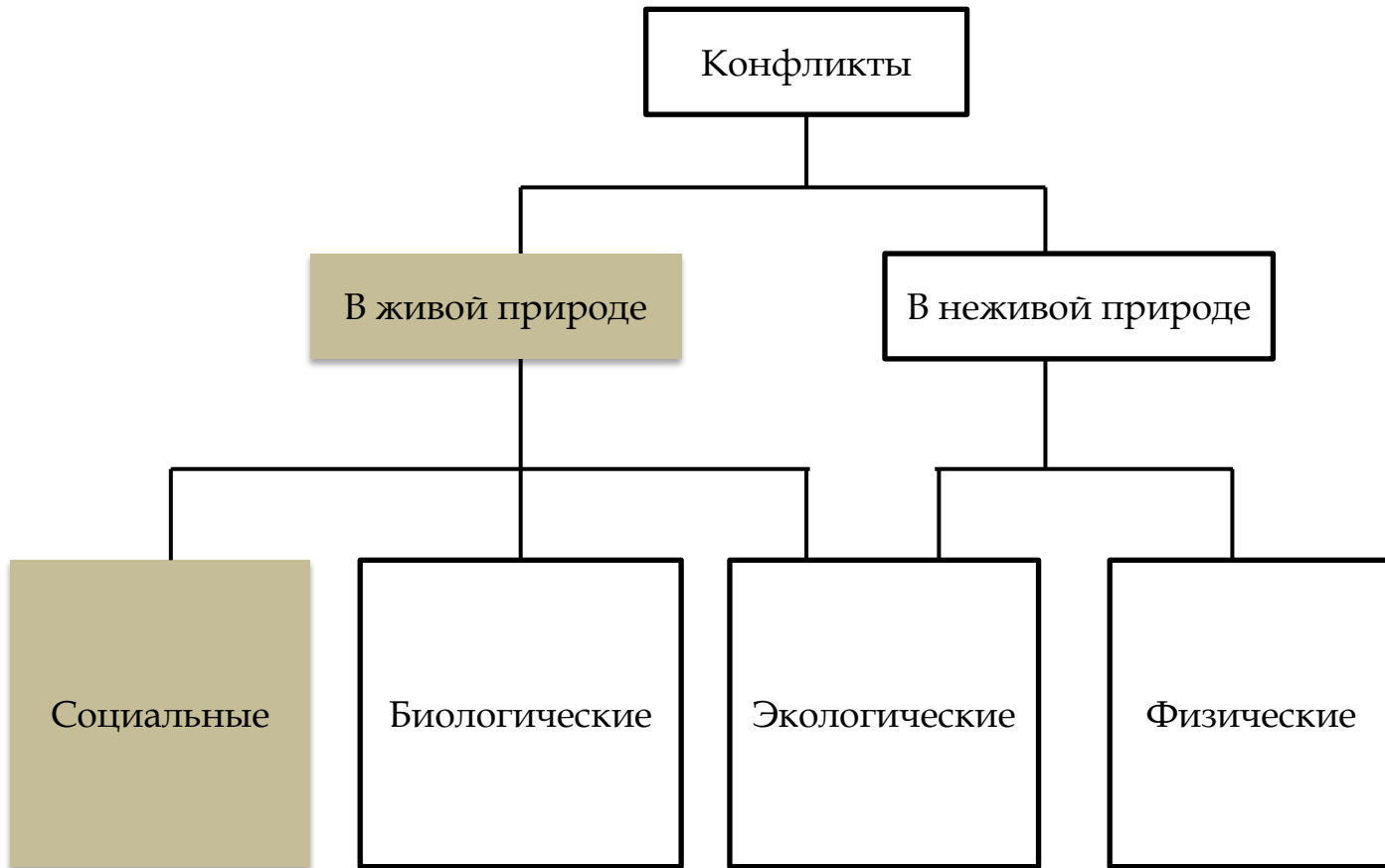
Основные функции системы безопасности



Зевс, Бог

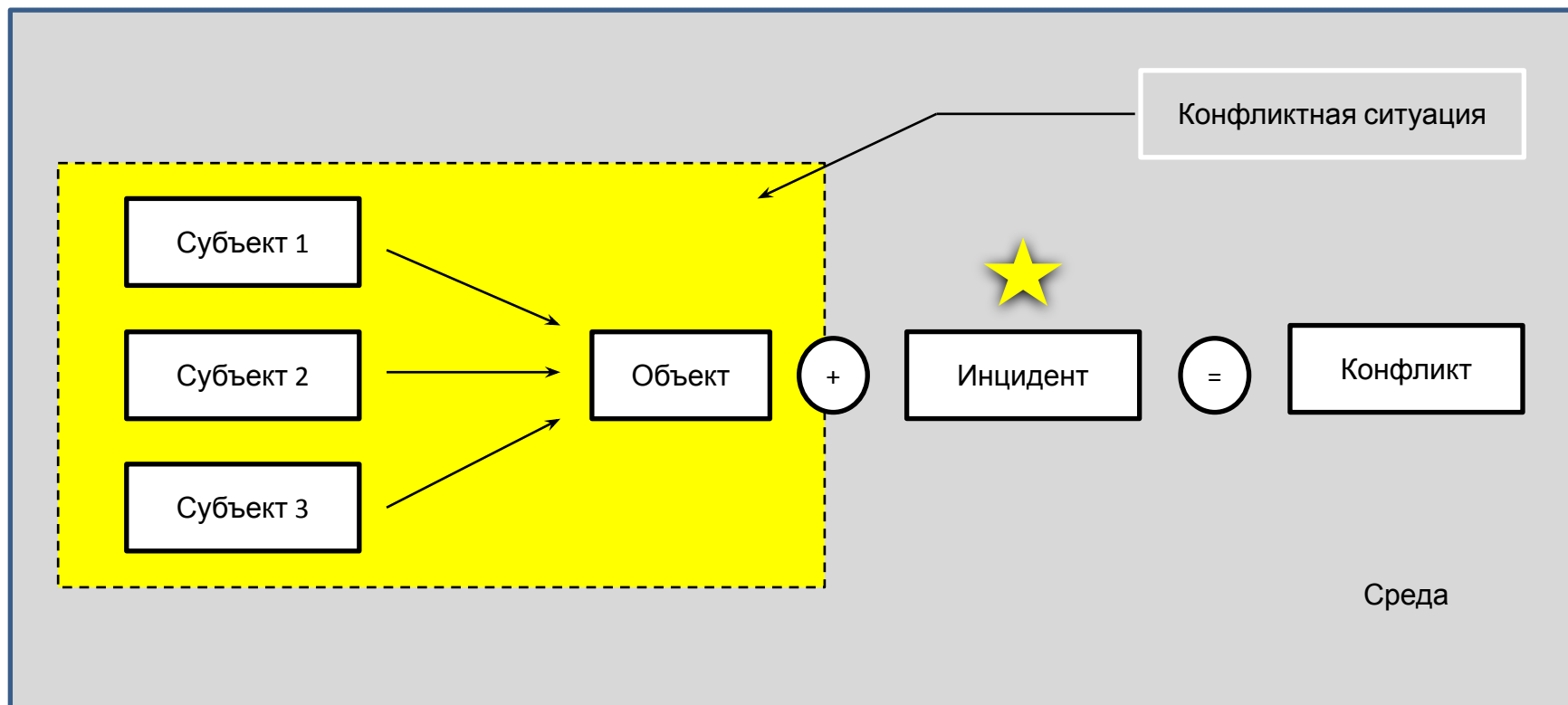


Общая классификация конфликтов по Новосельцеву В.И. и Тарасову Б.В.



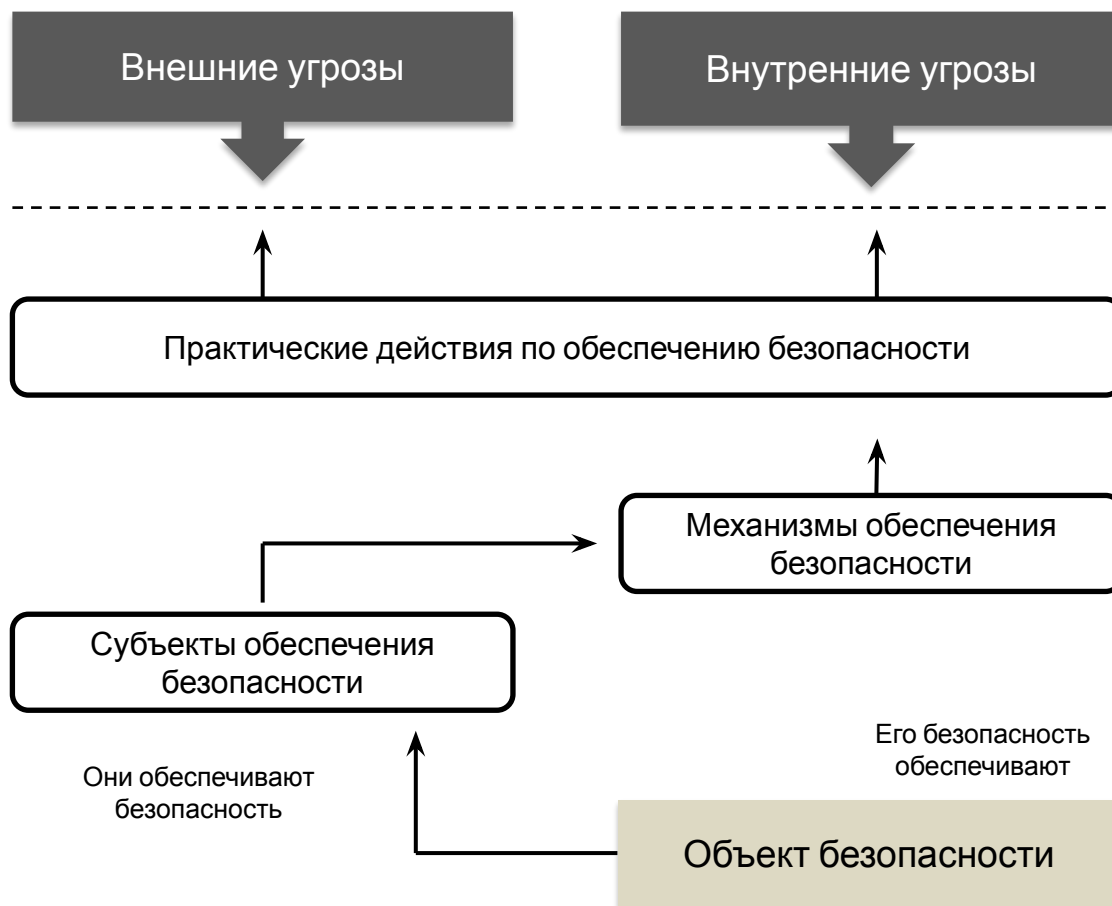
Методологически конфликт рассматривается в рамках структуры социального конфликта, предложенной Г.И. Козыревым*

*Политическая конфликтология. 2013, М., изд. «Форум», стр. 40





Структура функции обеспечения безопасности объекта:





Ключевые факторы современной внешней макросреды бизнеса:

1

Проблема
дефицита
информации

2

Условия
быстрых
перемен

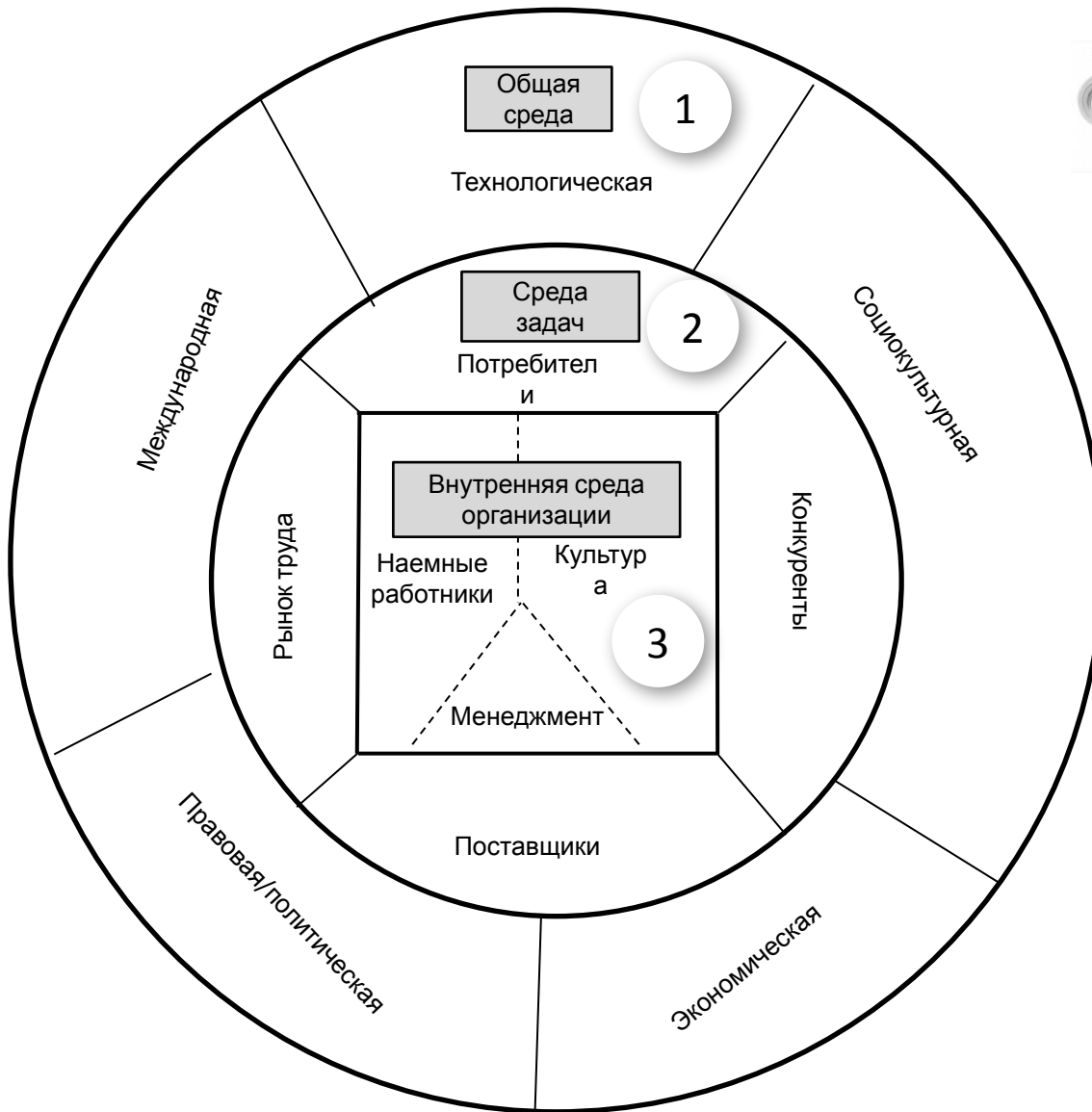
3

Эффект
глобализации

Осложняют реализацию функции безопасности!



Среда бизнеса:



Двухмерная
модель 1

Внешняя и внутренняя среда предприятия по Ричарду Дафту: Менеджмент



Поведенческая неопределенность:

Субъект оценки



**Рисковое
событие**

Очень субъективно

Необходимость ранжирования работников по занимаемому положению, знанию и опыту, типу мышления, умению контролировать свои действия и нести ответственность за их последствия...

Уровни факторов риска

- 1) Уровень фактора риска человеческой неопределенности внутренней среды организации
- 2) Уровень факторов риска человеческой неопределенности внешней микросреды компании
- 3) Уровень факторов риска природной неопределенности макросреды организации:
 - Нестабильность текущей экономической ситуации
 - Внешнеэкономический риск
 - Неопределенность политической ситуации
 - Неполнота или неточность информации о динамике или параметрах новой техники или технологии
 - Неопределенность колебаний рыночной конъюнктуры
 - Неопределенность природно-климатических условий
 - Неопределенность целей, поведения и интересов участников рынка
 - Неполнота или неточность информации о финансовом положении и деловой репутации участников рынка



Фактические материалы и статистика:

2011 г.

Ликвидирован
о

178 052



Предприятий-
банкротов

2012 г.

Ликвидирован
о

187 096



Предприятий-
банкротов

2013 г.

Ликвидирован
о

201 730



Предприятий-
банкротов

2014 г.

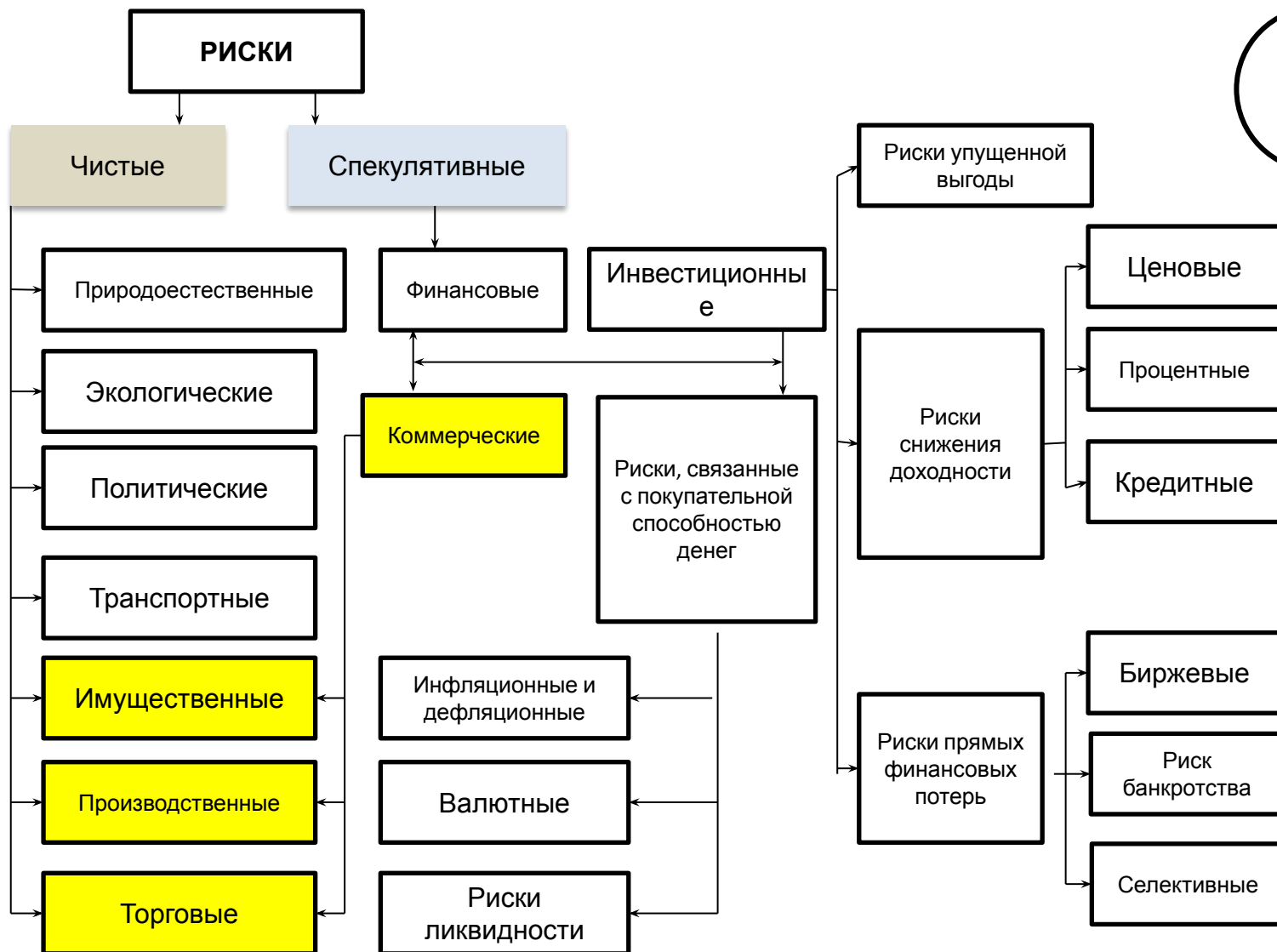
Ликвидирован
о

210 146

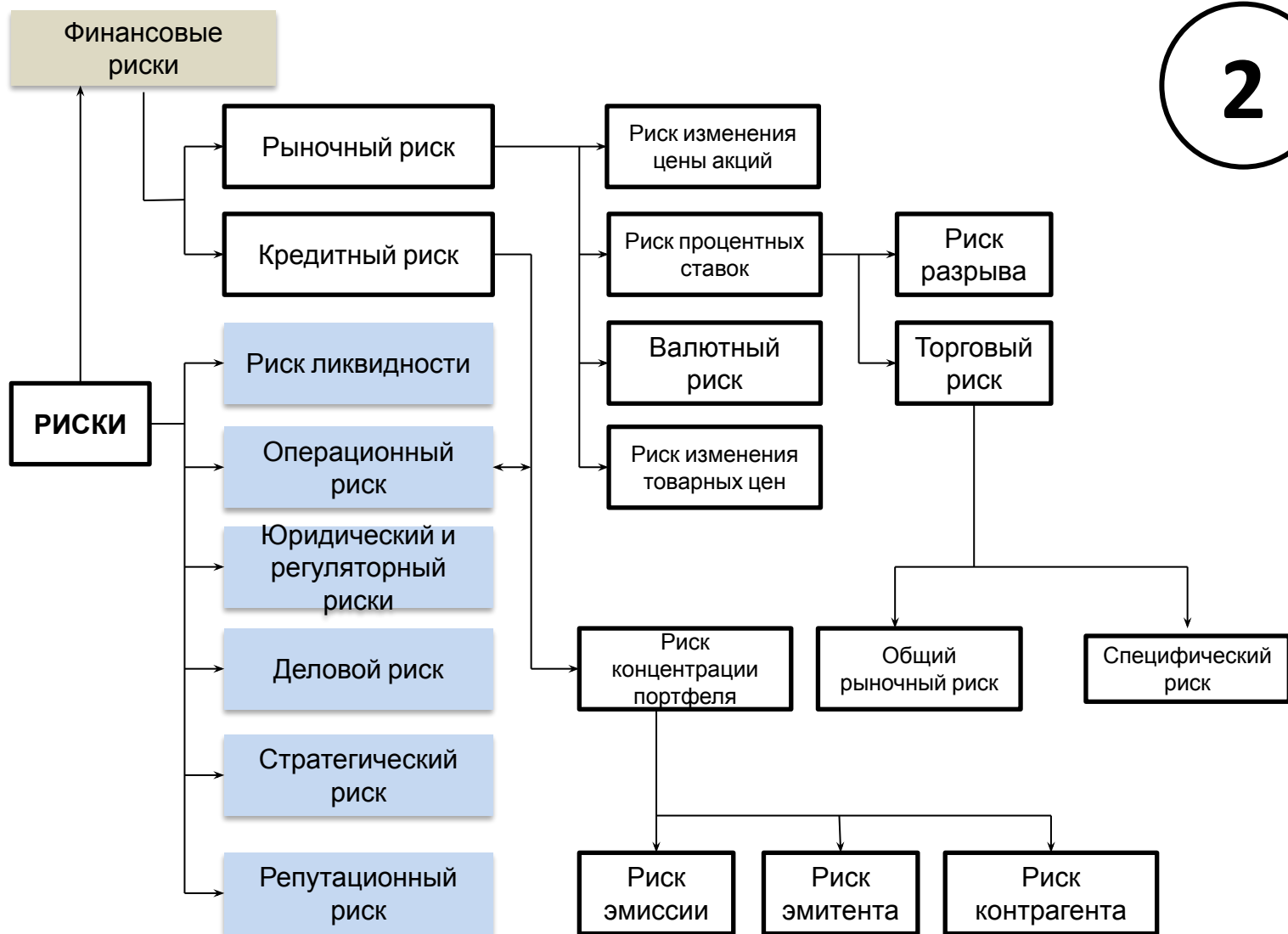


Предприятий-
банкротов

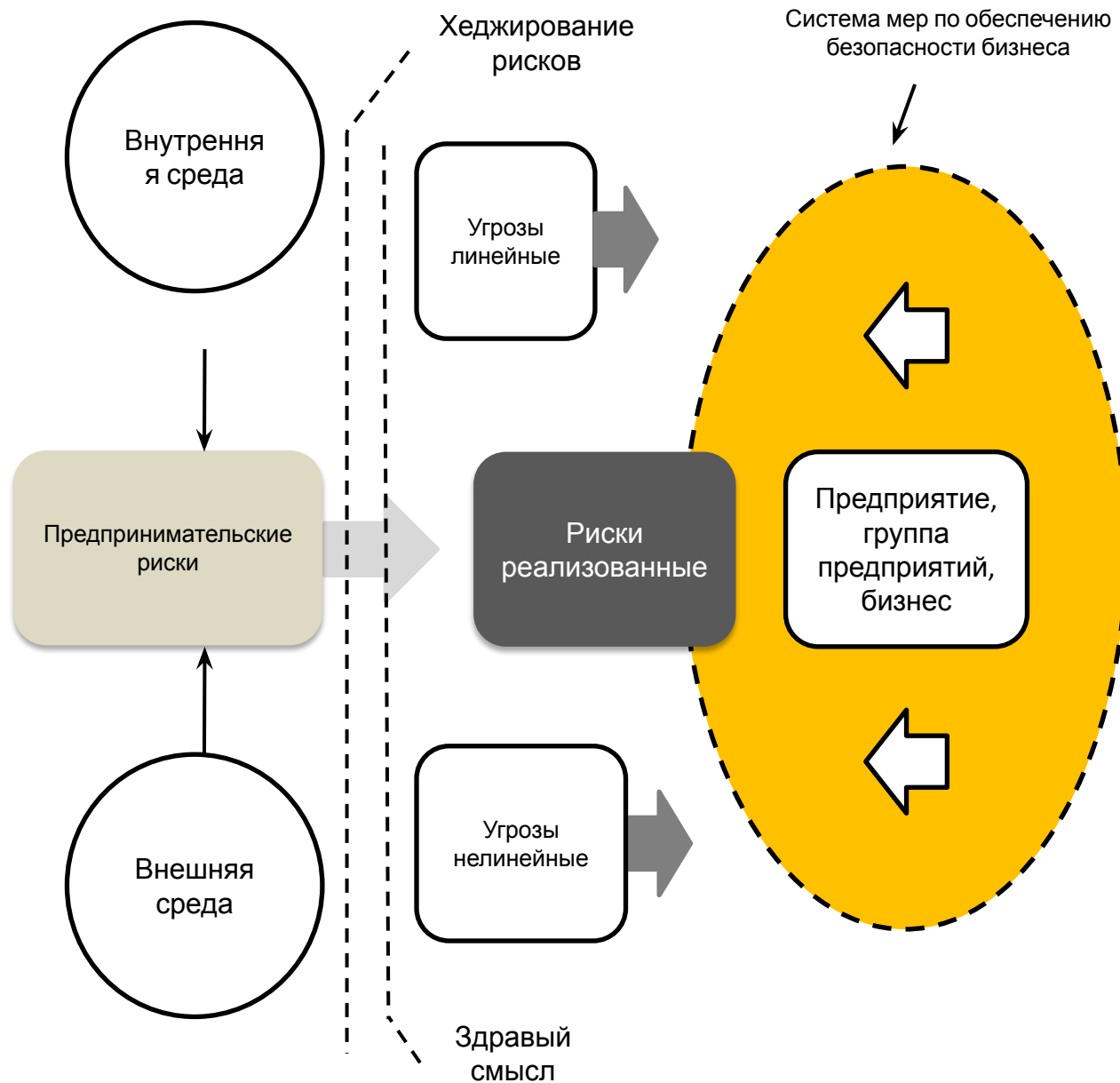
Без учета предприятий, понесших ущерб в следствие реализации рисков



Иерархическая система классификации хозяйственных рисков по Балабанову И.Т.



Иерархическая система рисков по М. Круи, Д. Галаю и Р. Марку



Соотношение рисков и угроз безопасности предприятия

Неэкономические риски:

Недобросовестная конкуренция

Коррупционные угрозы

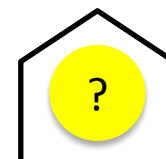
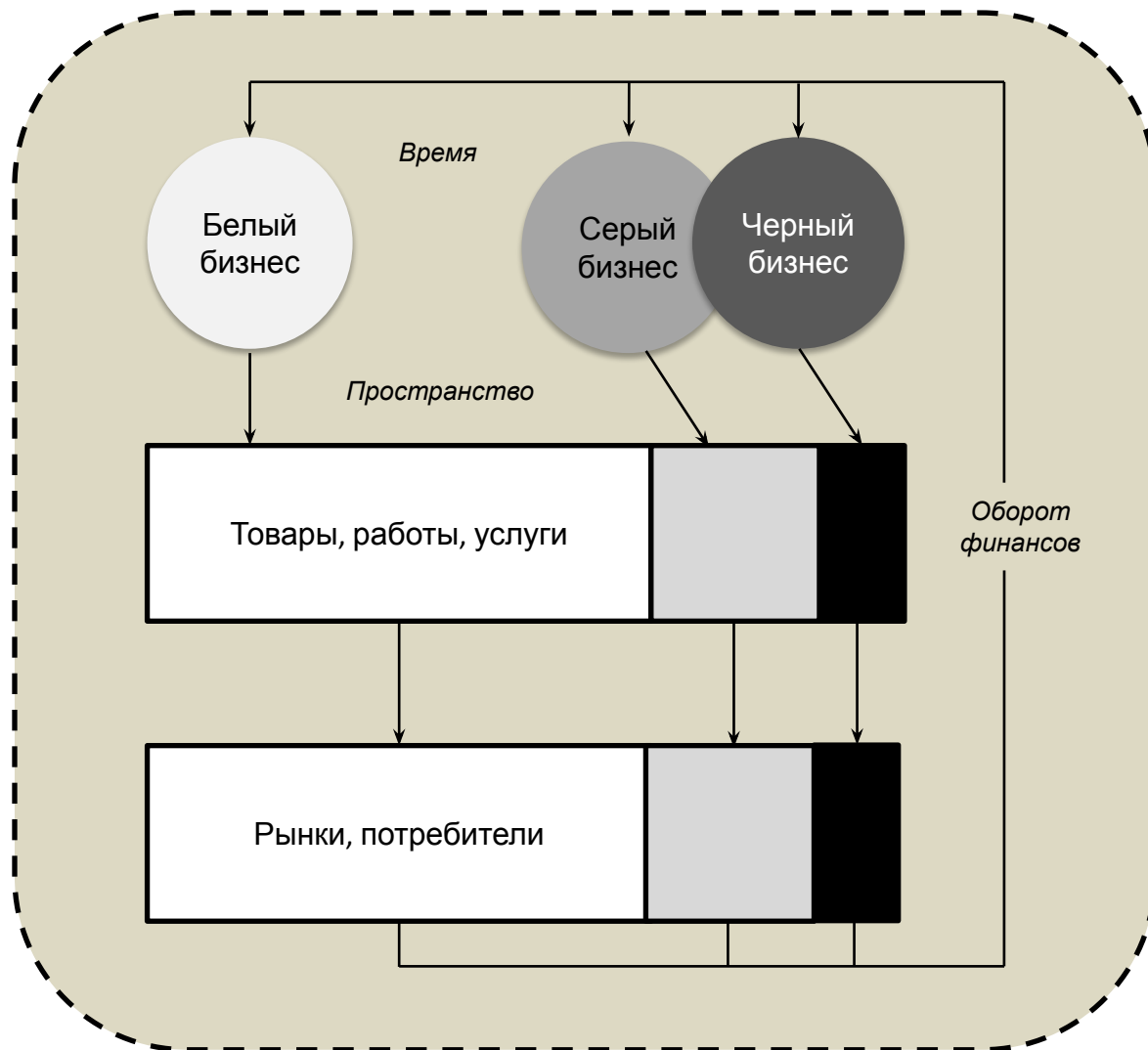
Вовлечение в систему теневой экономики

**Внутренние и внешние криминальные
угрозы**

**Использование запрещенных форм и
методов деятельности**



Финансовый оборот в легальном, полулегальном и нелегальном секторах экономики





Тюремная субкультура

Тюремная субкультура включает нормы, традиции, ритуалы, жаргон и жесты, принципиально отличные от тех, которые предполагает уголовно-исполнительное законодательство и внутренний распорядок тюрьмы.

Сообщество



Свои

Культурологические особенности

- Элементы клана
- Сетевая структура
- Персонификация отношений
- Отсутствие четких границ между сферами деятельности
- Несовершенство контроля над насилием
- Дуализм норм
- Незавершенная модернизация



Внешняя агрессивная среда



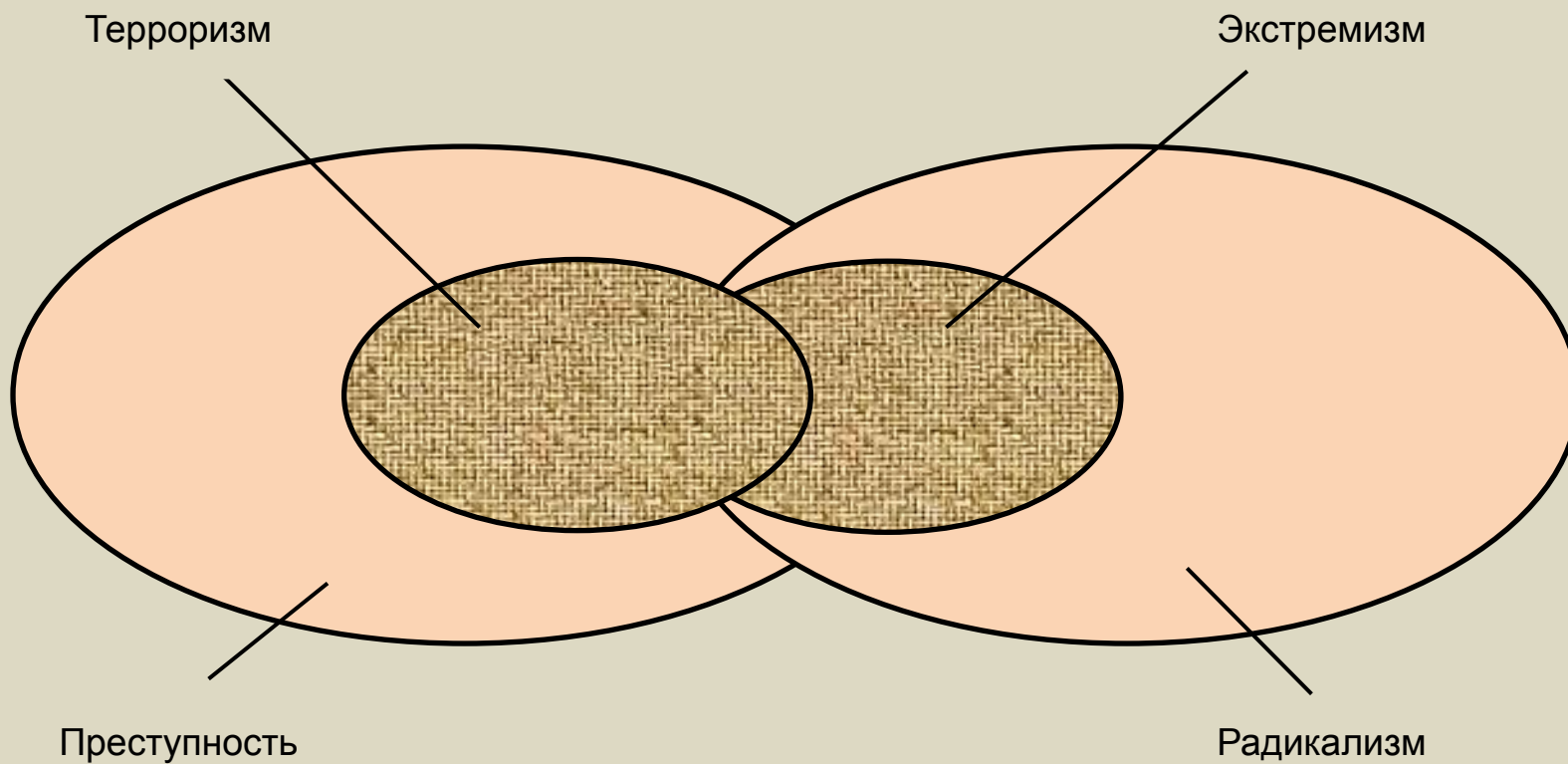
Чужие

Тотальные институты Гоффмана подразумевают солидарность внутри социальной группы и враждебность ее членов по отношению ко всему, находящемуся за ее пределами. «Теневая» жизнь существует и за стенами тюрьмы.

Дуализм в поведении и отношении членов «сообщества» (своих), с одной стороны, и тех, кто находится вне сообщества (чужих)



Соотношение экстремизма с терроризмом, радикализмом и общеуголовной преступностью



Экстремизм и его причины. Под редакцией Ю.
М. Антоняна. 2013. М. Логос

Типовой логистический центр



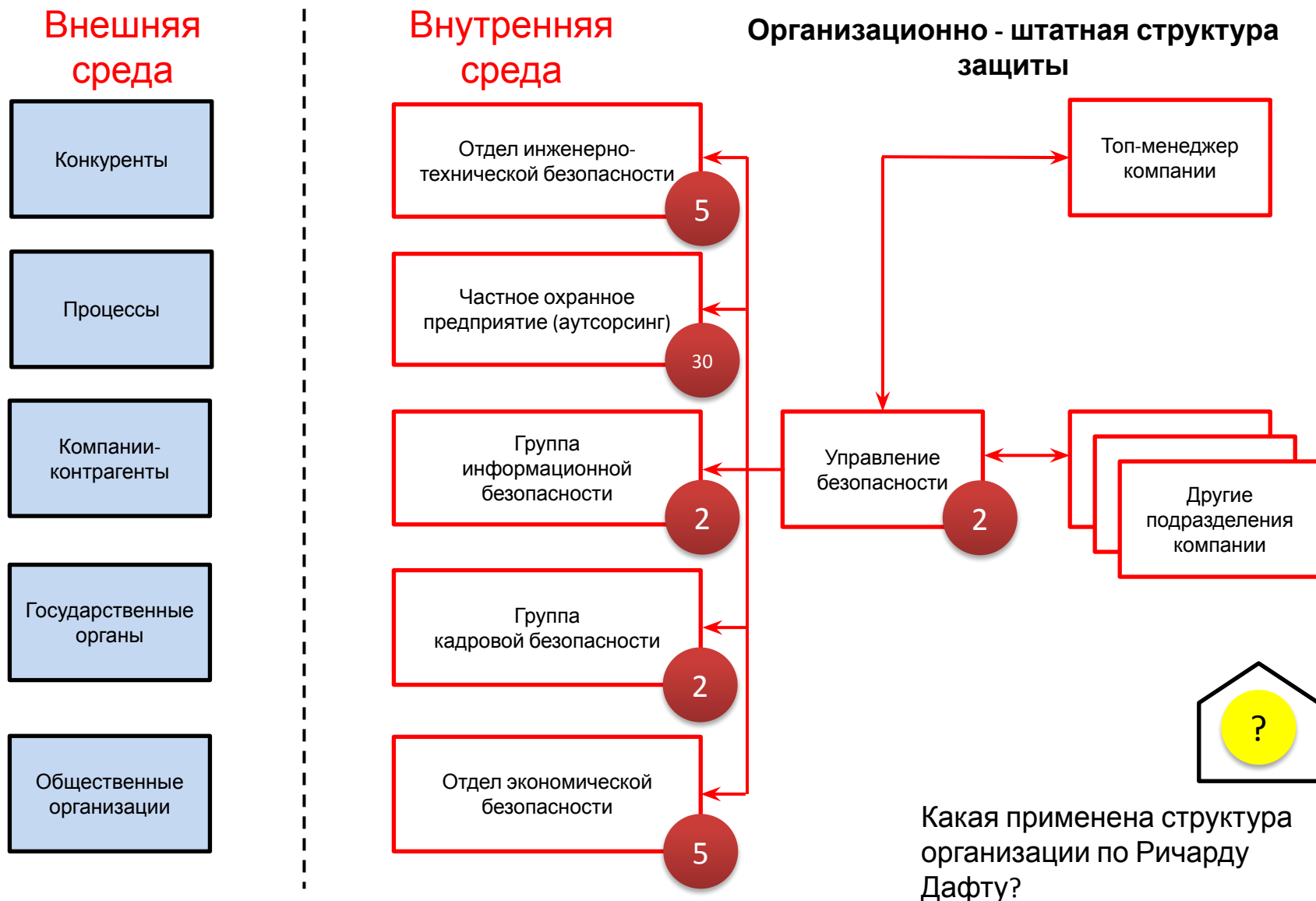
Описание:

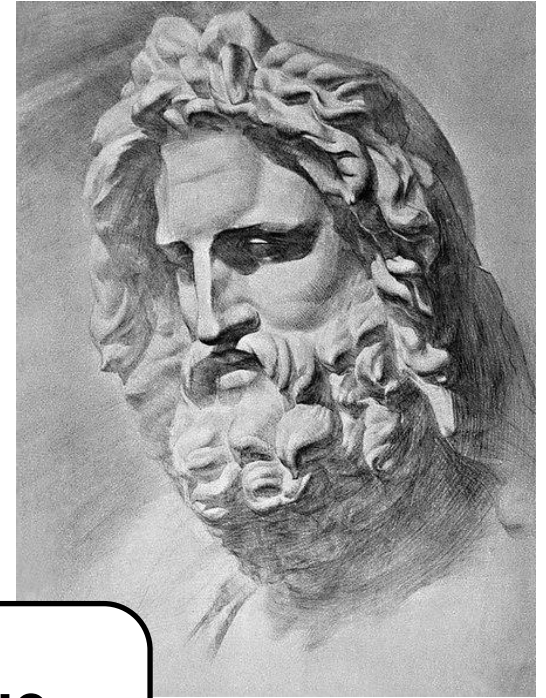
- крупный объект недвижимости;
- состоит из административного офиса и производственных помещений - нескольких терминалов, в некоторых из которых созданы специальные условия среды для определенных видов товаров;
- в каждом терминале имеются дорогостоящие основные средства: стеллажи, автоматизированная система погрузки и компьютерная система учета движения товара;
- общий объем находящихся на хранении товаров составляет до 20 млрд. руб., ежедневное движение товара (прием – отпуск) составляет не менее 200 млн. руб.
- в каждом терминале имеется несколько погрузочно-разгрузочных ворот;
- персонал состоит из 300 человек.

Примерная схема реализации штатной модели подразделения безопасности логистической компании в качестве ответа на реальные и потенциальные угрозы.



Примерная схема реализации организационно-штатной модели подразделения безопасности логистической компании в качестве ответа на реальные и потенциальные угрозы.





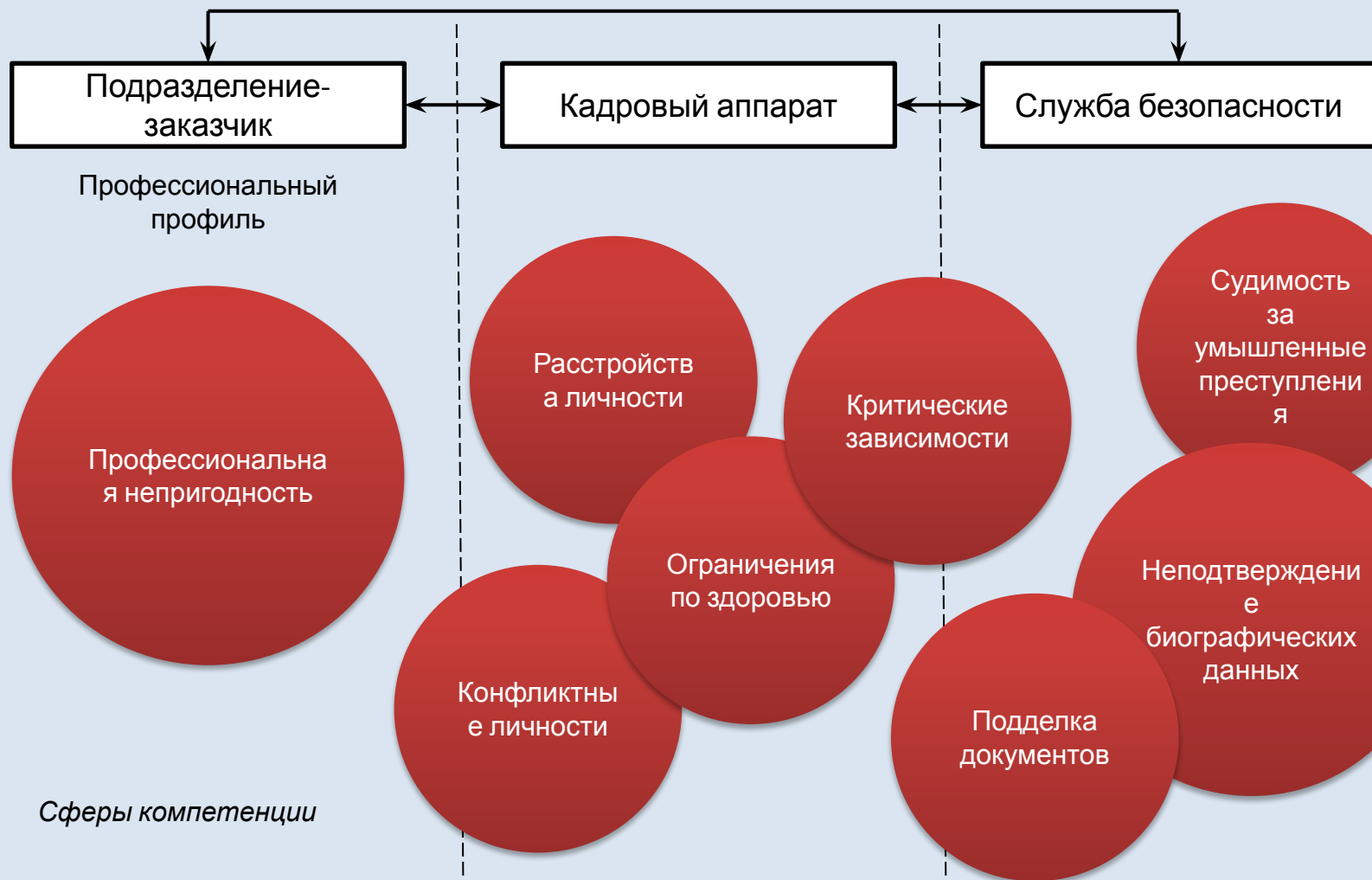
Связанные функции и пограничные области деятельности

Зевс, Бог

Группы риска

Критерии оценки фактов

Примерная типология

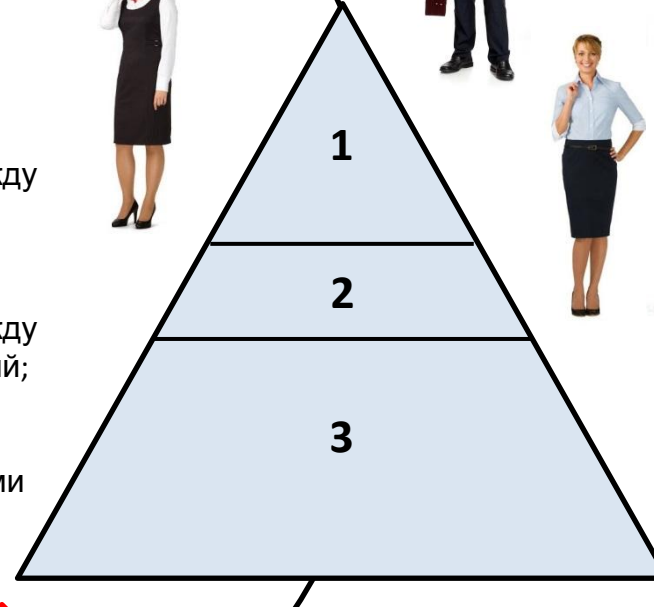


Внутренняя среда предприятия

Внешняя среда задач предприятия

- a. Маркетинг, реклама, PR;
- b. GR;
- c. Обмен информацией с общественными организациями;
- d. Неформальное общение между топ-менеджерами разных компаний по клубному принципу;
- e. Неформальное общение между работниками разных компаний;
- f. Формальное или неформальное общение работников с представителями внешней среды.

1. Начальники
2. Узкий контроль
3. Подчиненные



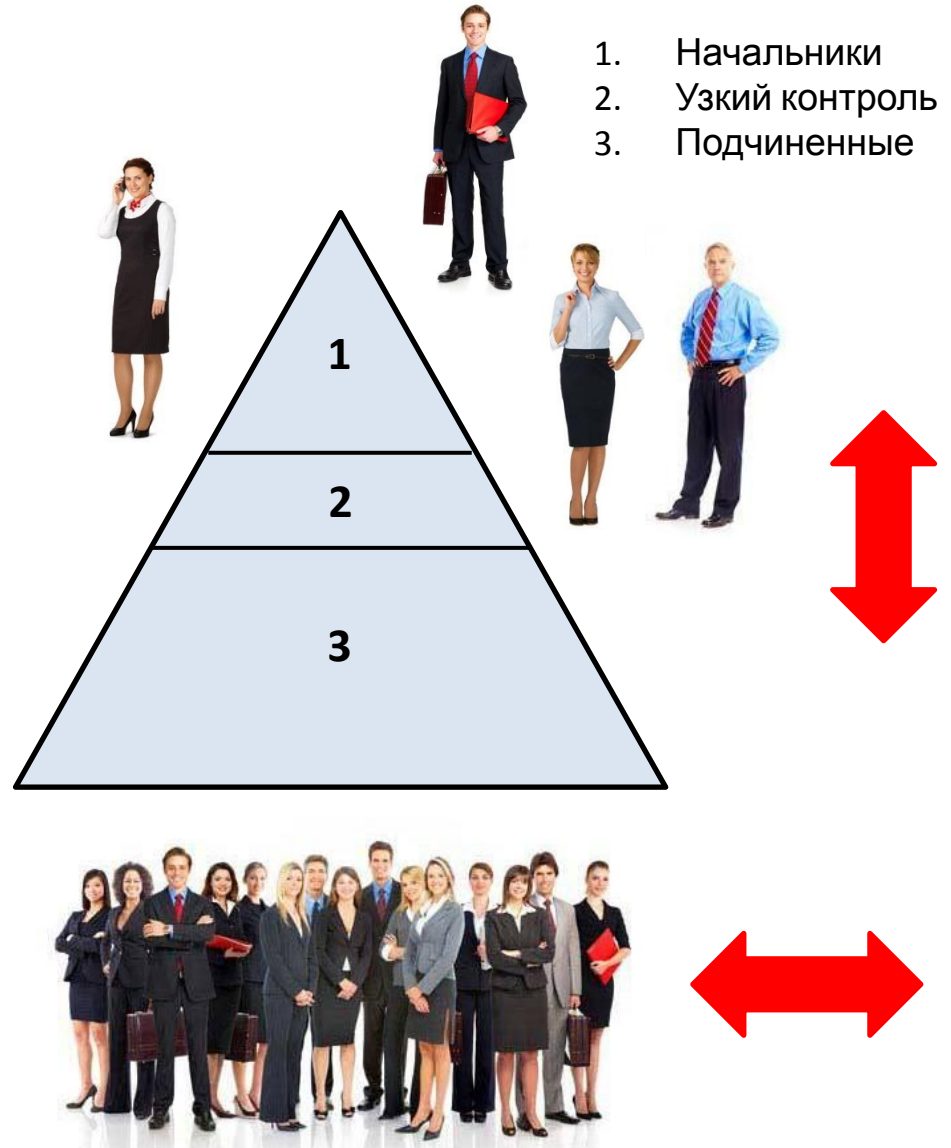
Внутренняя среда предприятия

Межуровневый обмен информацией внутри организации:

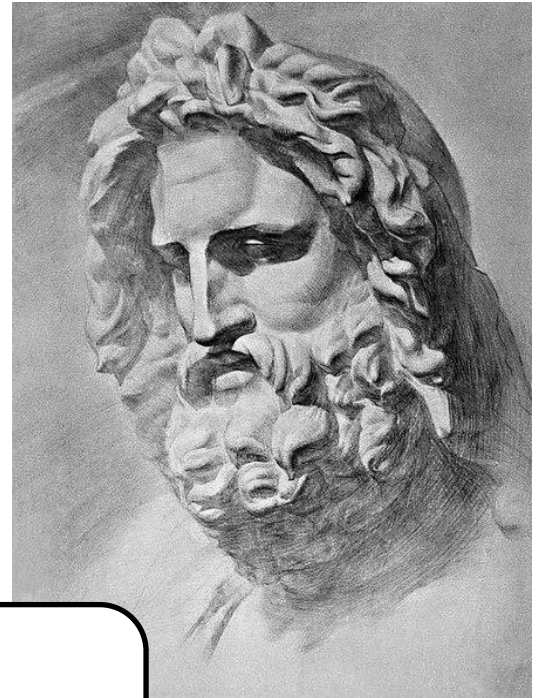
- a. Нисходящие потоки информации (решения органов управления, приказы, указания, инструкции, разъяснения, совещания, формальное и неформальное общение менеджеров с подчиненными);
- b. Восходящие потоки информации (отчеты о выполнении заданий, предложения по совершенствованию производства, жалобы на недостаточный уровень оплаты труда, предупреждения о проведении забастовок и иных акций протеста);
- c. Неформальное общение работников с менеджерами.

Горизонтальный обмен информацией:

- a. Совещания руководителей и специалистов взаимодействующих подразделений организации;
- b. Личное общение между руководителями и специалистами смежных подразделений в процессе рабочего взаимодействия;
- c. Неформальное общение между работниками одного предприятия;
- d. Смешанный тип неформальных коммуникаций (к примеру, циркулирование слухов).



Универсальность системы безопасности в рамках предприятия

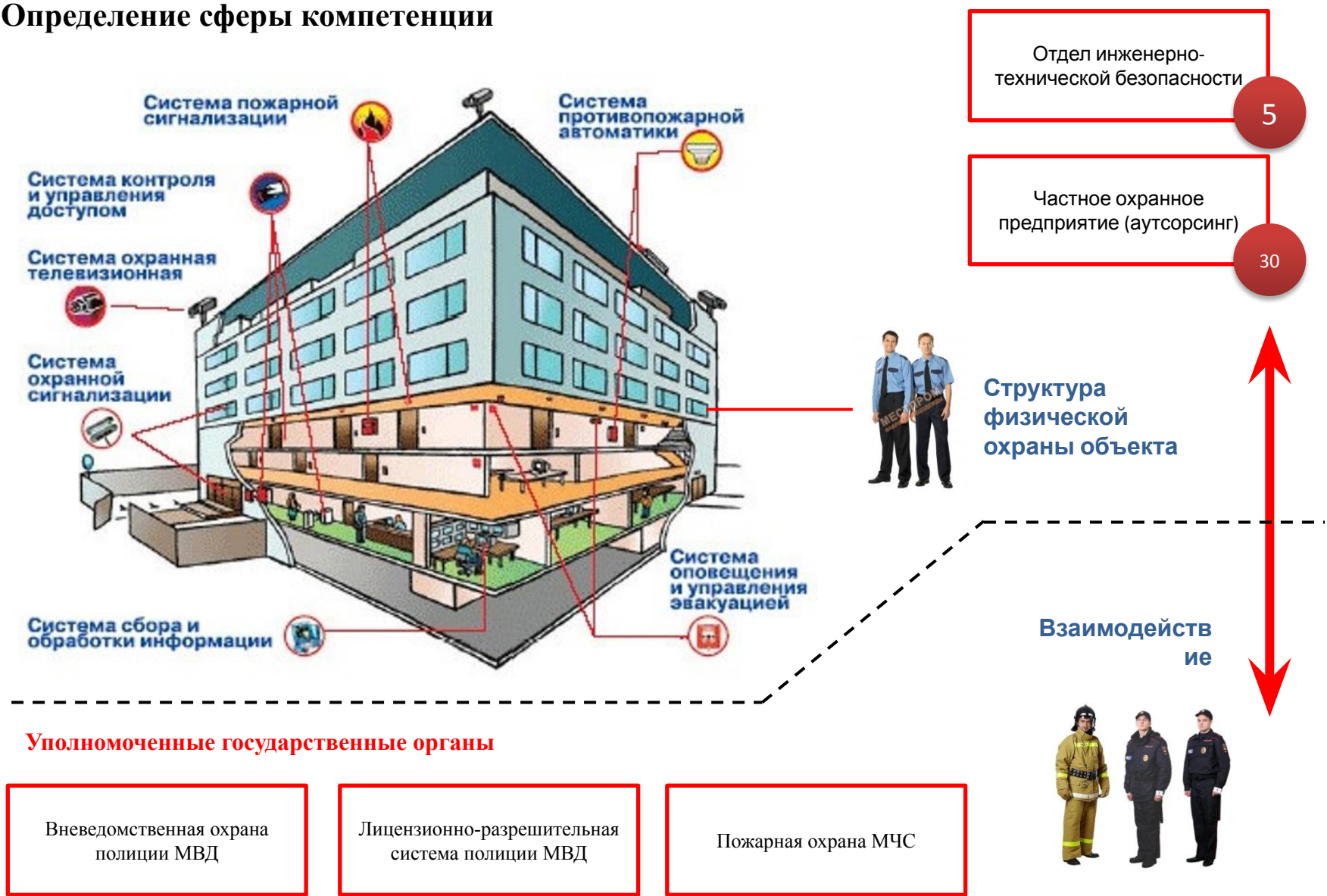


Зевс, Бог

Экономическая безопасность + средняя квалификация сотрудников + договор с бюро кредитных историй + наличие собственной базы данных - поверхностная проверка контрагентов - недоработки клиентских служб - отсутствие общего нормативного документа о порядке изучения потенциальных партнеров	Финансовая безопасность + высокая квалификация сотрудников + эффективный бухгалтерский контроль - нет функции внутреннего аудита - замечания от банка по нецелевому использованию кредита - выявлена попытка размещения на счете транзитных средств, подозрительная на отмывание Инженерно-техническая	Информационная безопасность + закуплено современное оборудование + установлены программные средства - нет подготовленных специалистов - функции автоматизации и ИБ не разделены - похищены средства с электронного счета компании - сотрудники используют ПК для игр в Интернете
Физическая безопасность + штаты охраны укомплектованы + сотрудники имеют лицензии + получено служебное оружие + сотрудники уверенно владеют штатными досмотровыми средствами - получены замечания по оборудованию оружейной комнаты - низкая профессиональная подготовка личной охраны генерального директора	безопасность + входы для работников оснащены СКУД + въезды оснащены средствами досмотра + периметр оснащен средствами контроля + склады оснащены средствами контроля - устарели средства видео-контроля - подлежат замене огнетушители - предписано автоматизировать средства пожаротушения в питейном цехе	Кадровая безопасность + утверждено положение о порядке подбора и изучения персонала + утверждено положение о порядке использования полиграфа + введена штатная должность оператора полиграфа + закуплен и введен в эксплуатацию полиграф - не выявлены организаторы схемы отмыкания денежных средств

Матрица SWOT-анализа для системы безопасности промышленного предприятия

Определение сферы компетенции

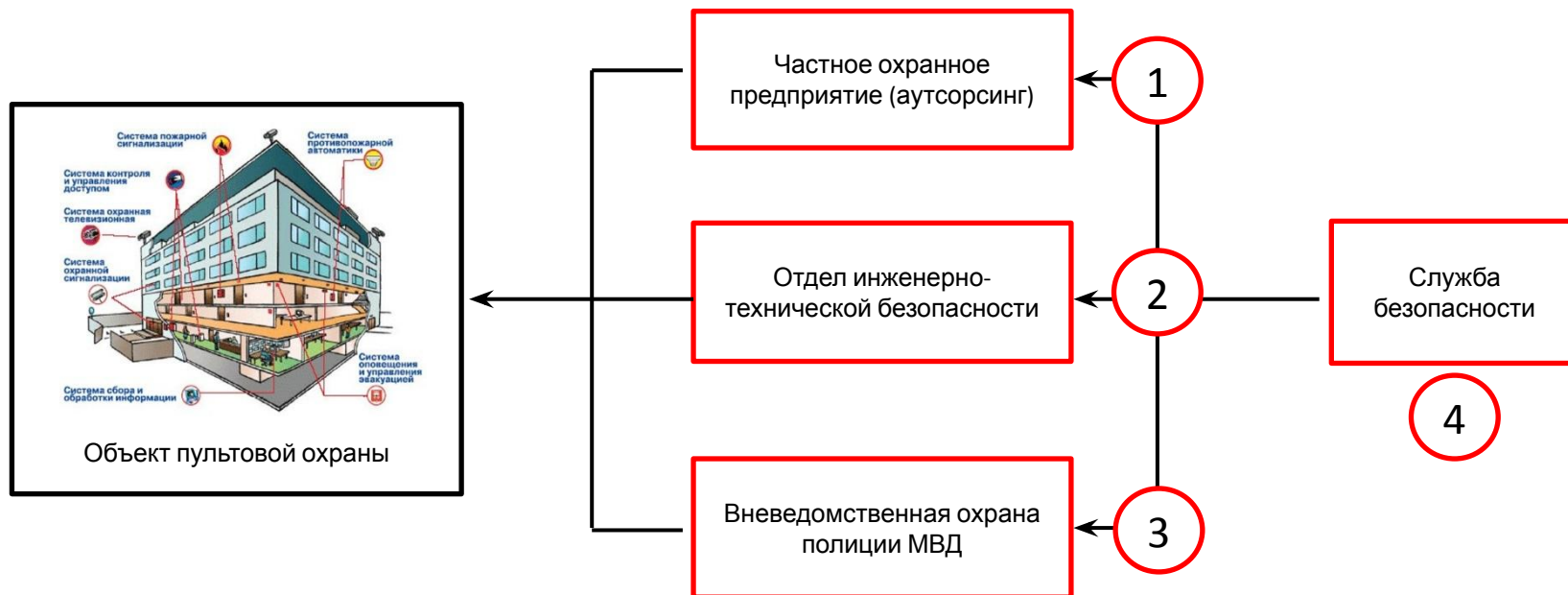


Действия полиции при охране объектов

- 1 – Пультовая охрана
- 2 – Выезд группы захвата по штатному сигналу тревоги
- 3 – При угрозе силового захвата выезд штурмовой группы
- 4 – При серьезной опасности выезд спецназа



«Сдержки и противовесы» (баланс интересов) при организации системы физической и инженерно-технической безопасности компании

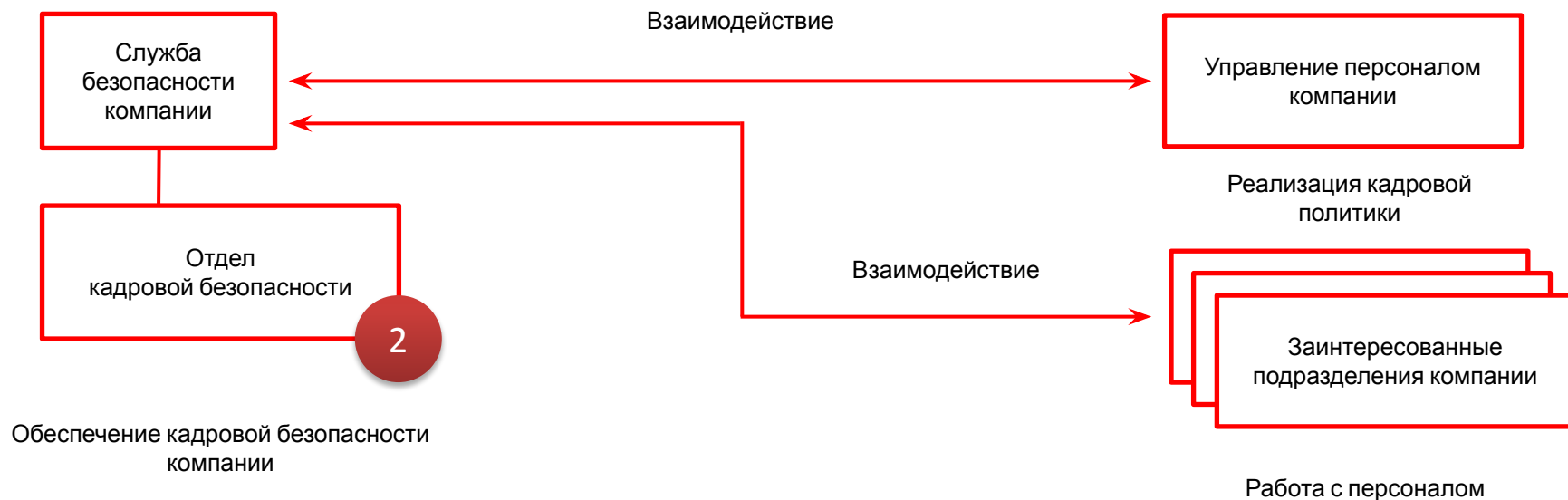


- 1) ЧОП по договору осуществляет физическую охрану объекта, пропускной и внутриобъектовый режим. При попытках несанкционированного проникновения на объект вызывает наряды полиции;
- 2) Отдел инженерно-технической безопасности (ИТБ) Управления безопасности компании осуществляет оборудование объекта техническими средствами, применяет и обслуживает данное оборудование, взаимодействует с вневедомственной охраной полиции и ЧОП в интересах компании;
- 3) Вневедомственная охрана полиции осуществляет техническую охрану объекта по договору через ПЦО, во взаимодействии с ЧОП и отделом ИТБ принимает необходимые меры реагирования;
- 4) Управление безопасности компании осуществляет управление, координацию и взаимодействие задействованных сил и средств в интересах защиты объекта от внутренних и внешних угроз.

Обеспечение информационной безопасности компании



Обеспечение кадровой безопасности компании



Противодействие коррупции изучение персонала на различных стадиях кадрового процесса:



А) при приеме



Б) в процессе работы



В) проведение
внутренних
служебных
расследований



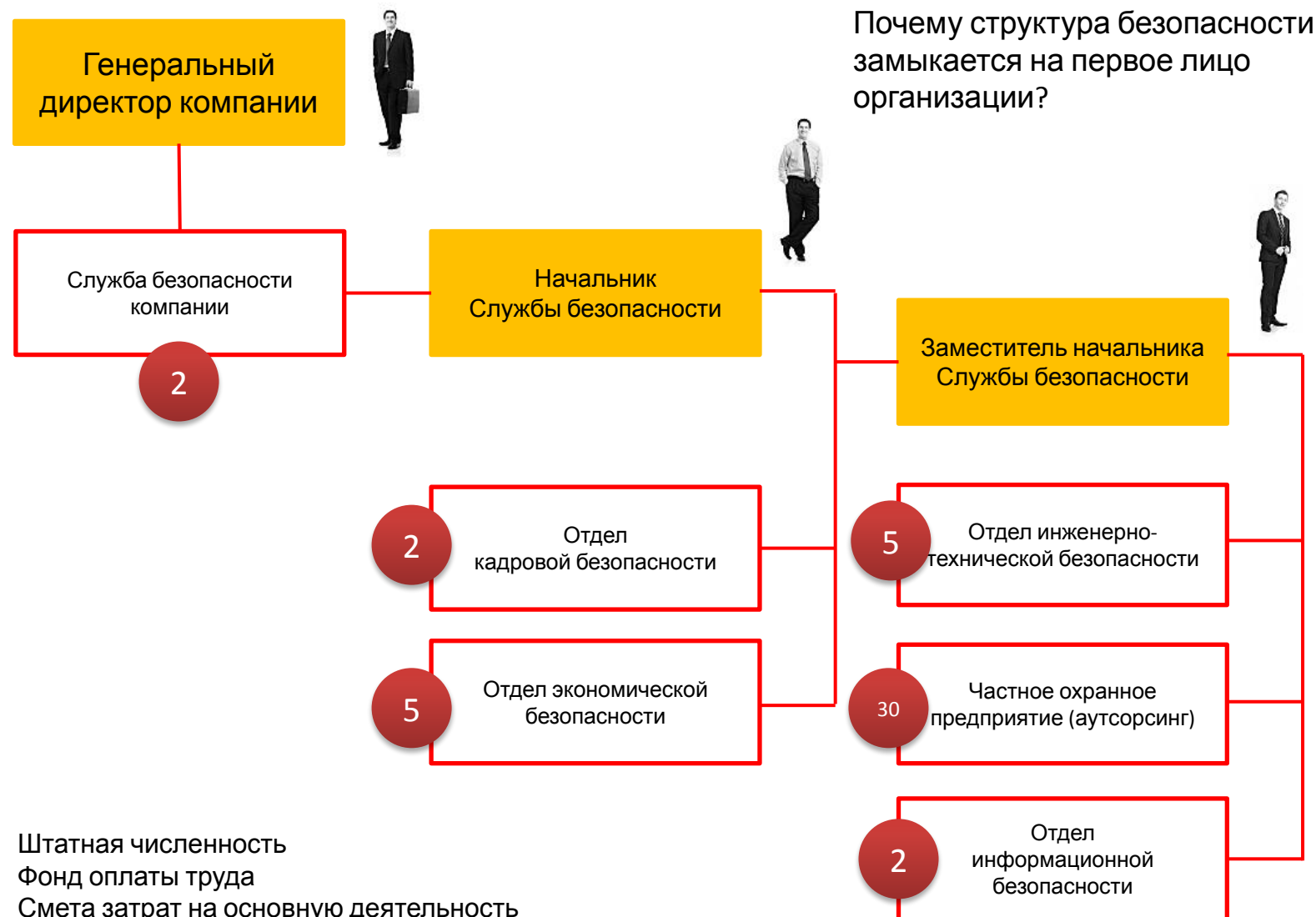
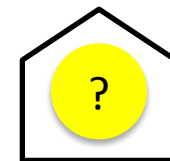
Г) при увольнении

**Уполномоченные
государственные органы**

Обеспечение экономической безопасности компании



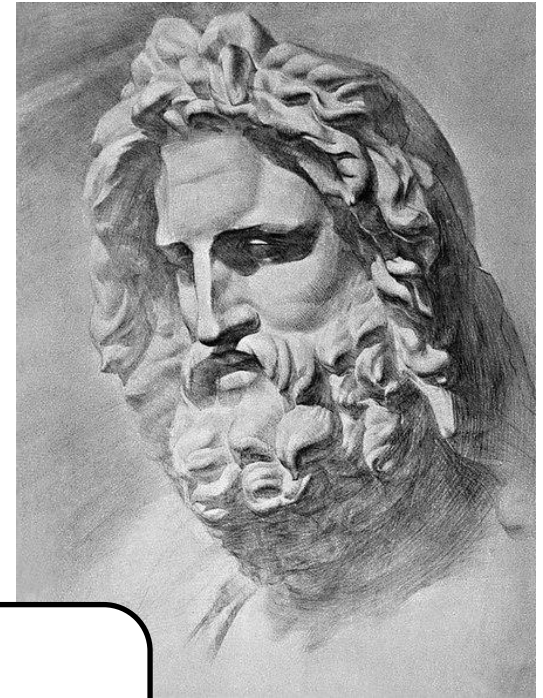
Обеспечение комплексной безопасности компании



Творческие подходы к построению систем безопасности

№	Наименование	Расшифровка
1.	Адекватность	Нецелесообразно «стрелять из пушки по воробьям» или «усекать голову в целях борьбы с перхотью»
2.	Оптимальность	Всегда целесообразно выбирать наиболее подходящий вариант защиты и нападения
3.	Достаточность	Сил должно быть достаточно, для того, чтобы остановить угрозу и создать комфортные условия для бизнеса
4.	Актуальность	Силы безопасности всегда необходимо поддерживать в состоянии соответствия новизне угроз: нет смысла с дубинками бросаться на танки, или стрелять из лука по пролетающему лазерному лучу.
5.	Динамичность	Статика – Стагнация - Смерть
6.	Профессиональность	Квалификация сотрудников должна позволять с известной долей резерва соответствовать угрозам.
7.	Прогрессивность	Консерватизм и нежелание учиться у жизни очень быстро скажутся на результате деятельности.
8.	Понятность	Меры безопасности должны быть понятны руководству и партнерам
9.	Публичность	Служба безопасности должна самостоятельно представлять себя во внешней и внутренней средах
10.	Надежность	Служба безопасности и работающие в ней сотрудники должны заслуживать доверия

Принципы построения системы безопасности предприятия



Зевс, Бог

Модули системы безопасности



Как быть практикам?

Потенциальная система безопасности состоит из модулей. За каждым модулем стоит самостоятельный вид деятельности. Этот вид деятельности может быть характерен для выбранного вида бизнеса, а может не иметь к нему никакого отношения. Каждый модуль состоит, в свою очередь, из подсистем, которые являются относительно самостоятельными отраслями того или иного вида деятельности.

Избранные для защиты конкретного бизнеса функции безопасности всегда должны соответствовать тем реальным и потенциальным угрозам, специфически характерным для каждого конкретного случая.

Размер и структура самой службы безопасности должна быть адекватной предприятию, в котором она создается, быть оптимальной и содержащей все функции (в своей структуре или на аутсорсинге), которые соответствуют сфере бизнеса.

Следует избегать соблазна создавать структуру не от функций, а под конкретного руководителя.

В последнее время в бизнесе принято называть должности своих сотрудников так, чтобы они позволяли им эффективно выполнять как внешние, так и внутренние функции.

По этой причине в небольшой компании может быть вице-президент по вопросам безопасности, а в крупной – директор департамента корпоративной защиты.

С академической точки зрения...



Считаем необходимым подчеркнуть еще раз:

- угроза – первична
- функция обеспечения безопасности – вторична
- название, структура, численность службы безопасности – третичны, четвертичны и пятиричны

Не менее важны системность, комплексность, мультипликативность.

Стадия мониторинга угроз

ТМ

топ менеджер,
коллегиальный орган

Принятие решения

ESM

менеджер
безопасности

Оценка информации
и выработка
решения

Реализация
решения

Угрозы внешней
среды

Угрозы внутренней
среды

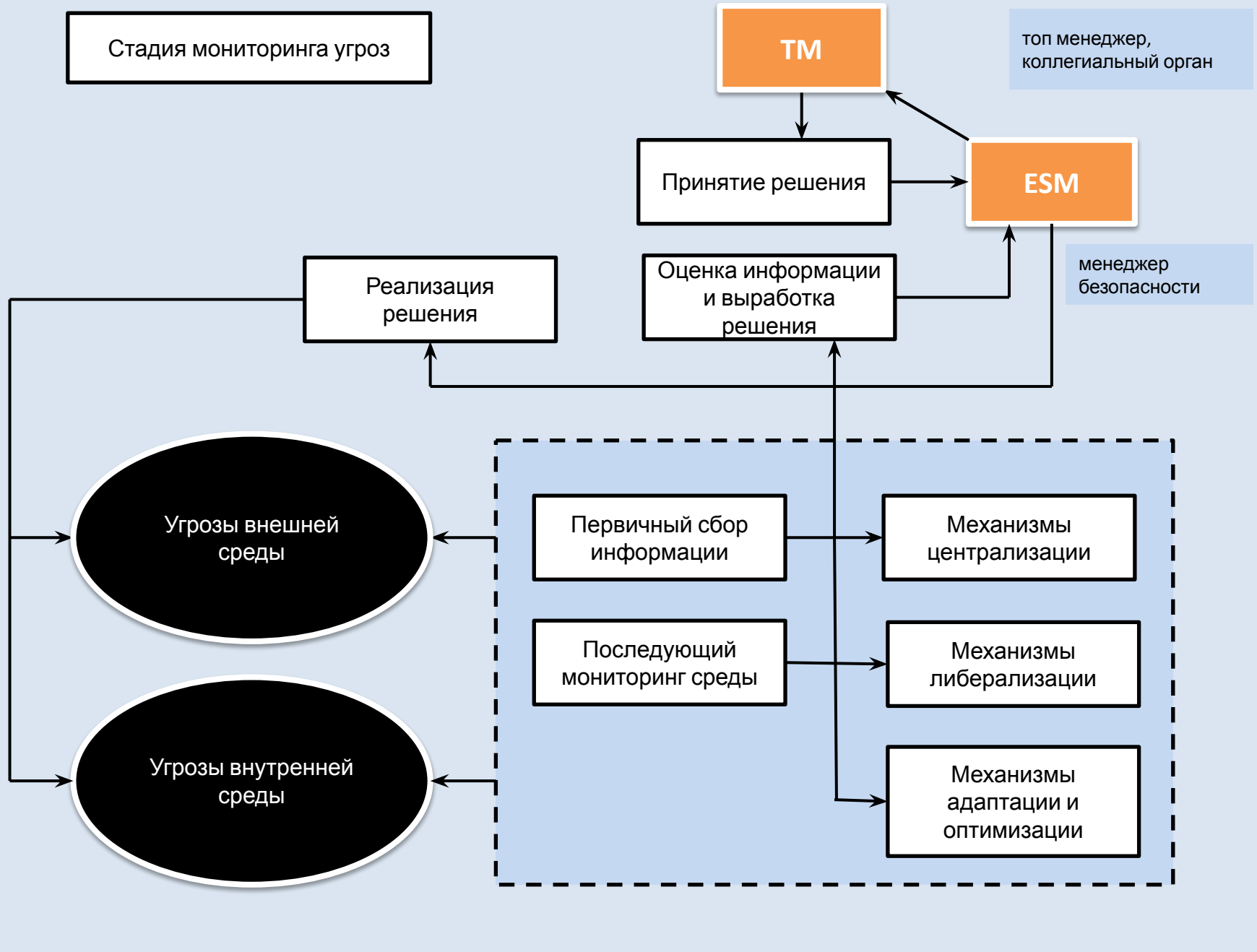
Первичный сбор
информации

Механизмы
централизации

Последующий
мониторинг среды

Механизмы
либерализации

Механизмы
адаптации и
оптимизации



Стадия декомпозиции угрозы

Пример

ESM

1 – Виды охраняемых сведений

Угроза разглашения охраняемых сведений

ТМ

Формы, методы и способы преодоления защитных мер

Система мер по обеспечению безопасности охраняемых сведений

Виды охраняемых сведений

Тайна персональных данных
(физических лиц)

Банковская тайна
(в соответствии с законом)

Налоговая тайна
(юридических и физических лиц)

Коммерческая тайна
(контрагента по договору)

Государственная тайна
(по выполняемому контракту)

Коммерческая тайна
(собственная)

Менеджмент систем безопасности

ESM

TM

2 – формы хранения охраняемых сведений

Формы, методы и способы преодоления защитных мер

Система мер по обеспечению безопасности охраняемых сведений

Формы хранения охраняемых сведений

В электронной базе данных

В форме материальных образцов

На съемном электронном носителе

На кино-фото пленке

На бумажном носителе

В устной форме

Виды охраняемых сведений

Менеджмент систем безопасности

ESM

TM

3 – меры защиты охраняемых сведений

Формы, методы и способы преодоления защитных мер

Система мер по обеспечению безопасности охраняемых сведений

Организационные меры

Правовые меры

Режимные меры

Физические меры

Инженерно-технические меры

Программно-аппаратные меры

Формы хранения охраняемых сведений

Виды охраняемых сведений

Менеджмент систем безопасности

Пример декомпозиции угроз:
4 – меры преодоления защиты

ESM

TM

Путем несанкционированного съема
электронными средствами

Путем превышения полномочий третьими
лицами

Путем хищения / копирования с носителей

Путем несанкционированного съема
техническими средствами

Путем выведывания у инсайдеров

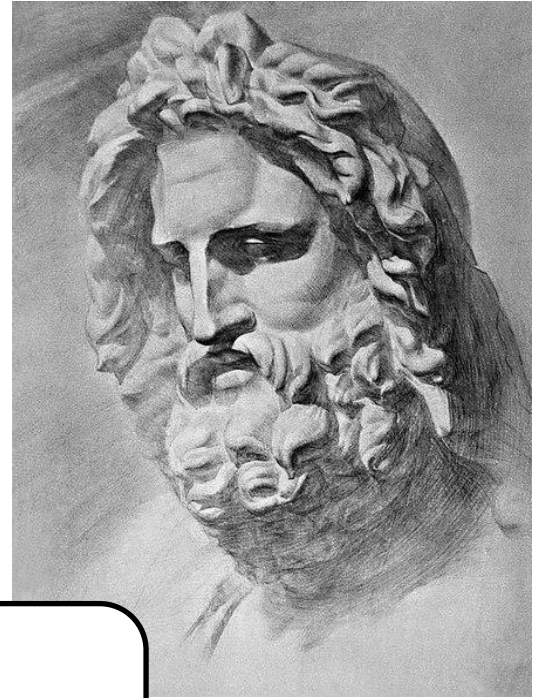
Путем подкупа инсайдеров

Формы, методы и способы преодоления защитных мер

Система мер по обеспечению безопасности охраняемых сведений

Формы хранения охраняемых сведений

Виды охраняемых сведений



Библиография

Зевс, Бог

Основная литература

1. Шульц В.Л., Рудченко А.Д., Юрченко А.В. Безопасность предпринимательской деятельности. Часть 2. М.: изд. Юрайт. 2016, С 145-200.

Литература для продвинутых студентов

1. Дафт Р. Теория организации. М.: изд. Юнити. 2012;
2. Дафт Р. Менеджмент. 8-е издание. М.-СПб.: изд. Питер. 2011;
3. Джейли Дж.А., Рени Ф.Дж. Микроэкономика. М.: изд. НИУ ВШЭ. 2011.