



Организация и методики проведения плановых проверок

Практическое занятие № 1.

Организационно-методические подходы к созданию системы плановых проверок.

Власенко М.Н.

Доцент кафедры «Безопасности и информационных технологий», к.э.н., профессор РАЕ.

Организация и методика проведения плановых проверок.

Цель, задачи, методы.....

Общая информация по дисциплине:

Объем дисциплины:	108 часов
Лекции:	32 часа (16 занятий)
Практическая работа:	32 часа (16 занятий)
Самостоятельная работа:	44 часа

Экзамен с оценкой.

Общая оценка за экзамен + результаты работы в семестре (По 4-м промежуточным результатам БАРС) = оценка за дисциплину – в диплом!

Выступление с докладами на практических занятиях.

На оценку «5» - 5 и более раз в семестр.

На оценку «4» - 4 раза в семестр.

На оценку «3» - 2-3 раза в семестр.

Индивидуальные письменные отчеты по семинарским занятиям (4 практические задания).

Домашнее творческое задание в конце семестра.

«Организация и методики проведения плановых проверок»- как наука, призвана помочь специалистам, занимающимся обеспечением безопасности ХС, ответить на вопросы:

- *Как можно оценить степень безопасного функционирования организации?*
- *Как выявлять злоупотребления и мошенничество?*
- *Какие признаки опасности существуют?*
- *Чем должны заниматься должностные лица и подразделения в ходе контрольно-проверочных мероприятий?*
- *Какова цена предложенных мероприятий?*
- *На сколько эффективно реализована предложенная система безопасности?*
- *Каким образом сократить затраты на безопасность не снижая ее уровень? На чем можно сэкономить?*
- *Какой способ финансирования того или иного проекта более предпочтителен и почему?*
- *Как убедить руководителя предприятия в том, что потраченные средства на безопасность целесообразны и какой будет от этого эффект?*
- *Какова величина возможного ущерба в случае отказа от реализации предложенной системы безопасности?*
и ряд других....

**Как экономически оценить
эффективность системы контроля и
управления информационной и
экономической безопасностью?**

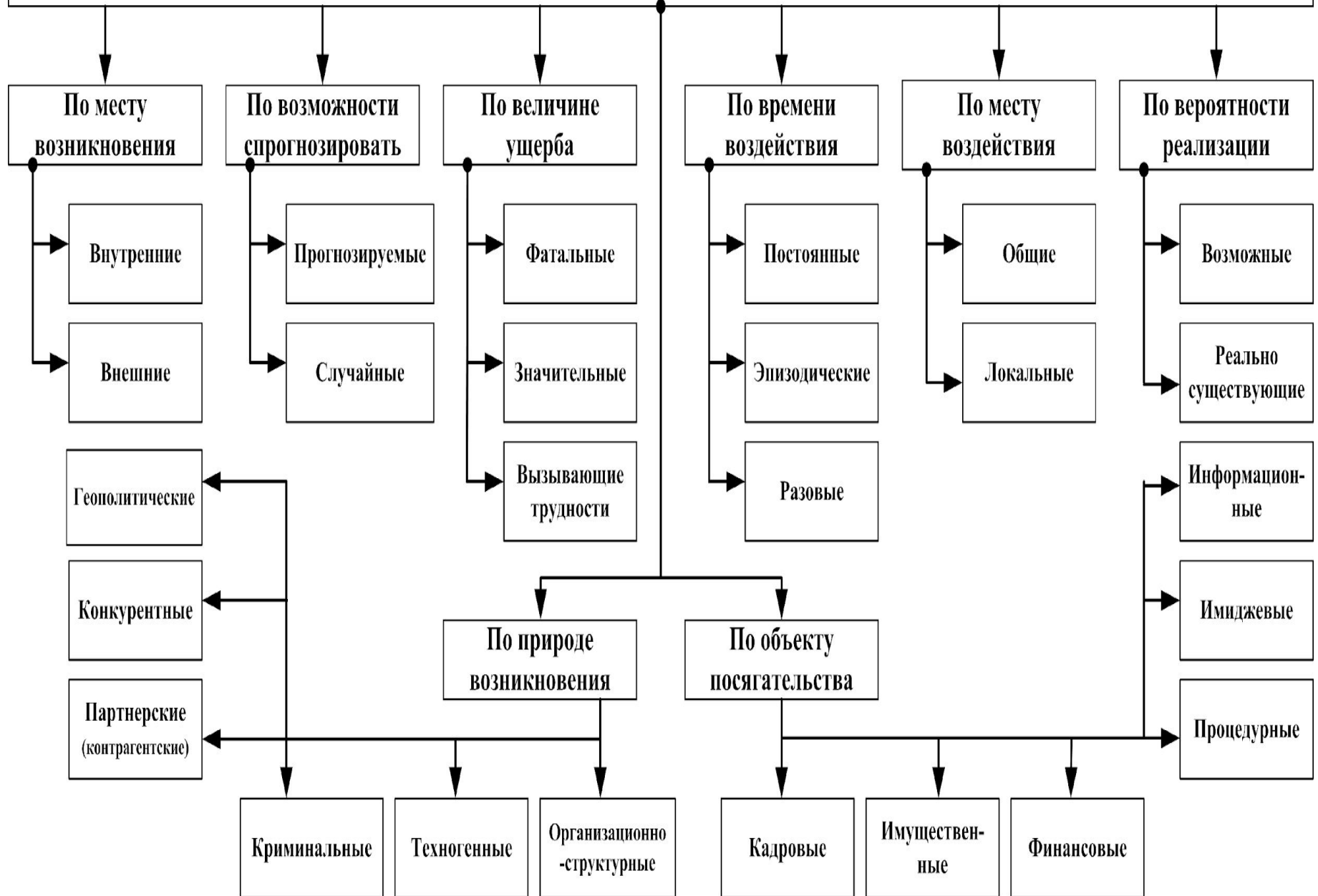
**Как эффективно управлять объектом
защиты для снижения последствий
реализации угроз?**

Угрозы и риски: сходства и различия?

**Как выявить недостатки в системе управления и
злоупотребления персоналом?**

- **Подсистема контрольно-ревизионной деятельности-**
составная часть системы
экономической (информационной)
безопасности предприятия.

Классификация угроз экономической безопасности по направлениям



Риск-факторы организации внутреннего происхождения

Персонал

Технические средства охраны

Информационная система

Локальная вычислительная сеть

Экономическая система

Инженерно-технические системы

Финансы

Нормативно-правовое регулирование

Система физической защиты

Система защиты авторских прав

Система внутренней логистики

Система управления бизнес-процессами

Материально-техническая база

Система учета и контроля

Экология среды, производства,
продукта

Адаптивность к изменениям

Внешняя среда организации сложное многофакторное структурное образование включающее:

- трудовые ресурсы;
- демография;
- госрегуляторы, находящиеся на подведомственной территории и их структуры;
- криминальные элементы на территории расположения объекта;
- культура, мораль, традиции жителей по месту расположения объекта;
- профсоюзы, другие общественные организации, например, природоохранные, защищающие права местного населения;
- экономическая ситуация в регионе;
- общеполитические факторы;
- социальные факторы;
- международное окружение;
- принятая в регионе система налогообложения.

Риск-факторы организации внешнего происхождения

Госрегуляторы

Потребители

Контрагенты

Нормативно-правовая система
государства

Политическая система

Экономическая политика государства

География территории

Окружающий социум

Конкуренция

Криминал

Террористы

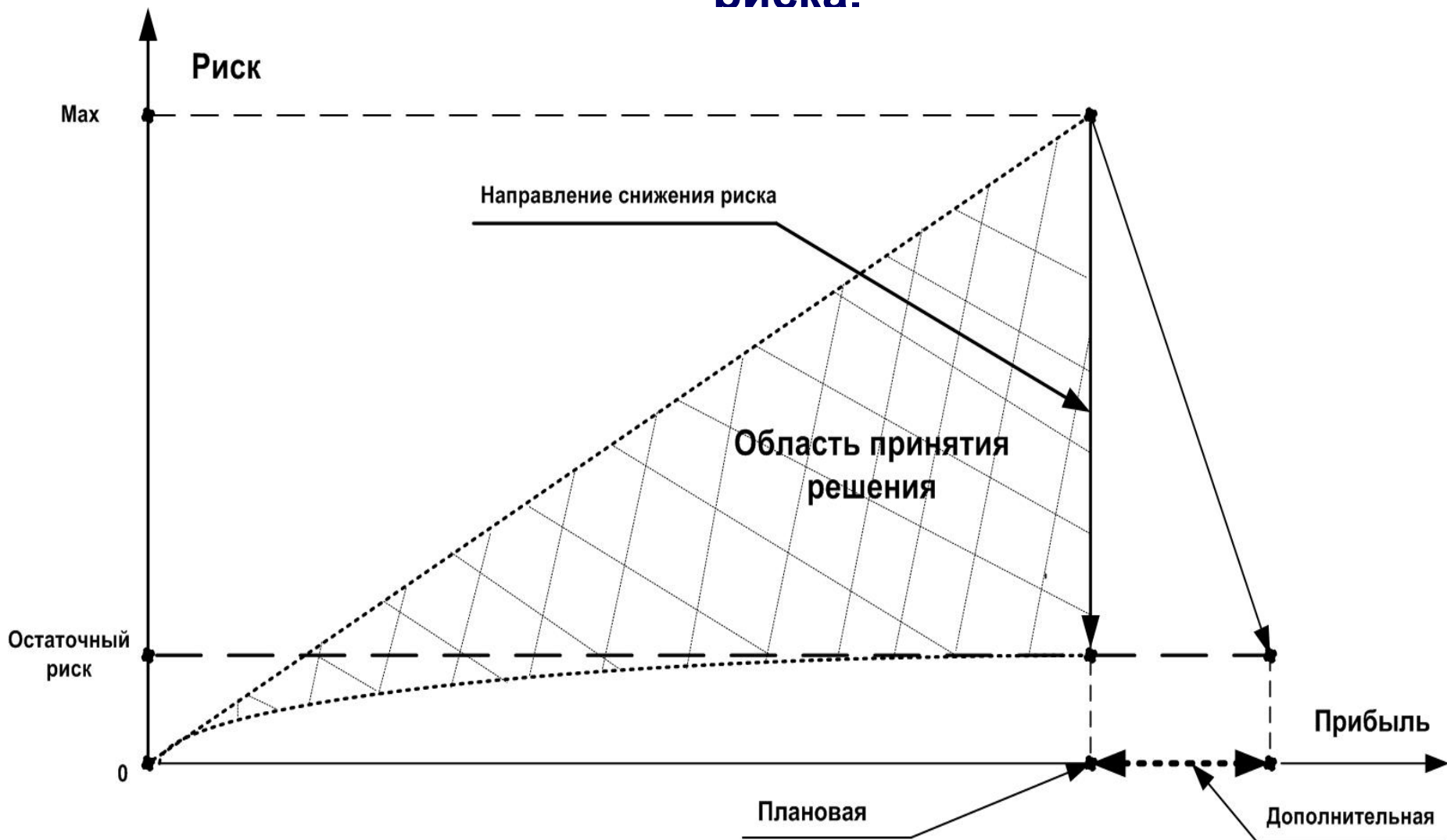
Техногенная, природная среда

Спрос

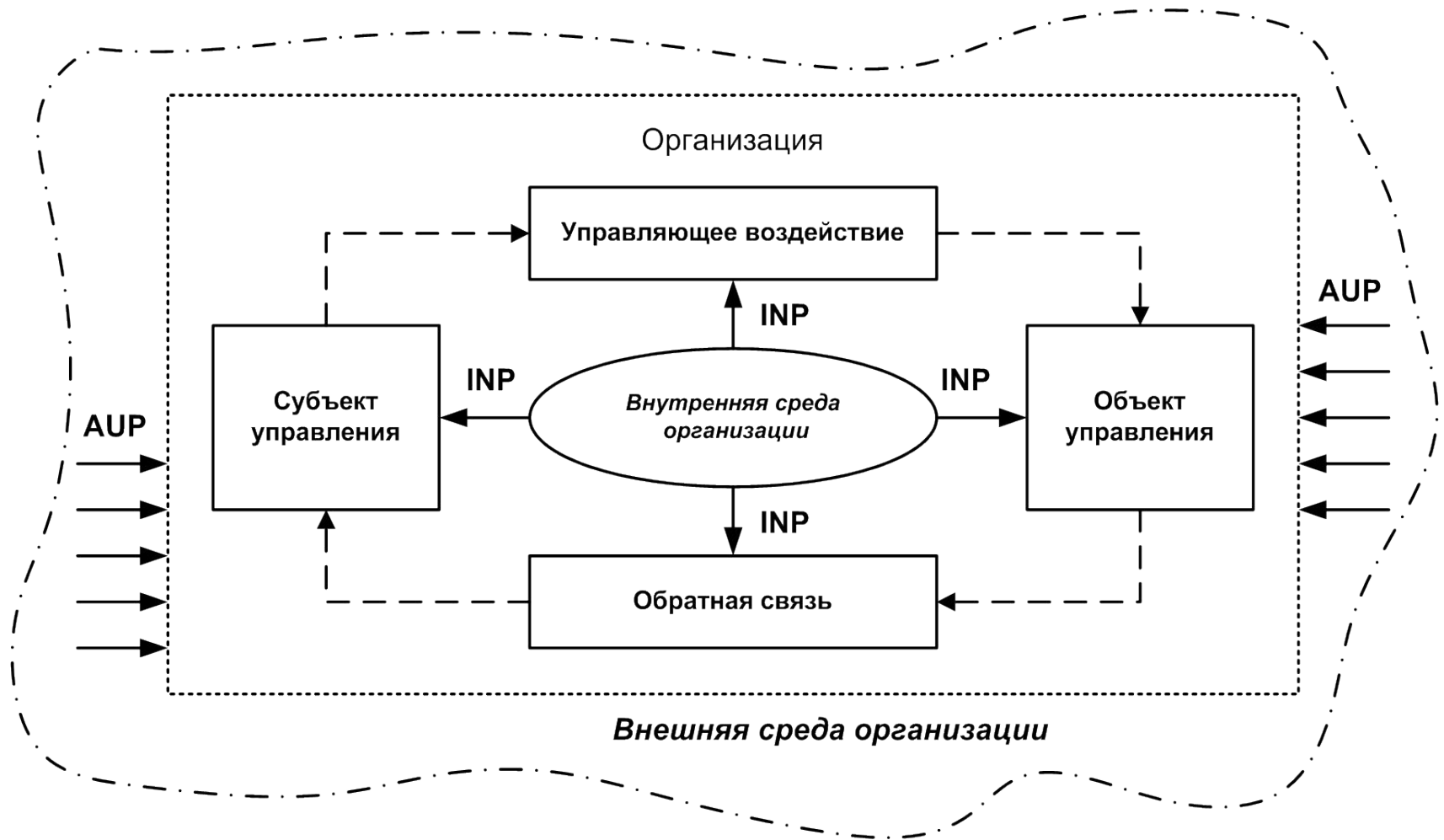
Уровень коррупции в регионе, стране

На сколько эффективно можно управлять рисками?

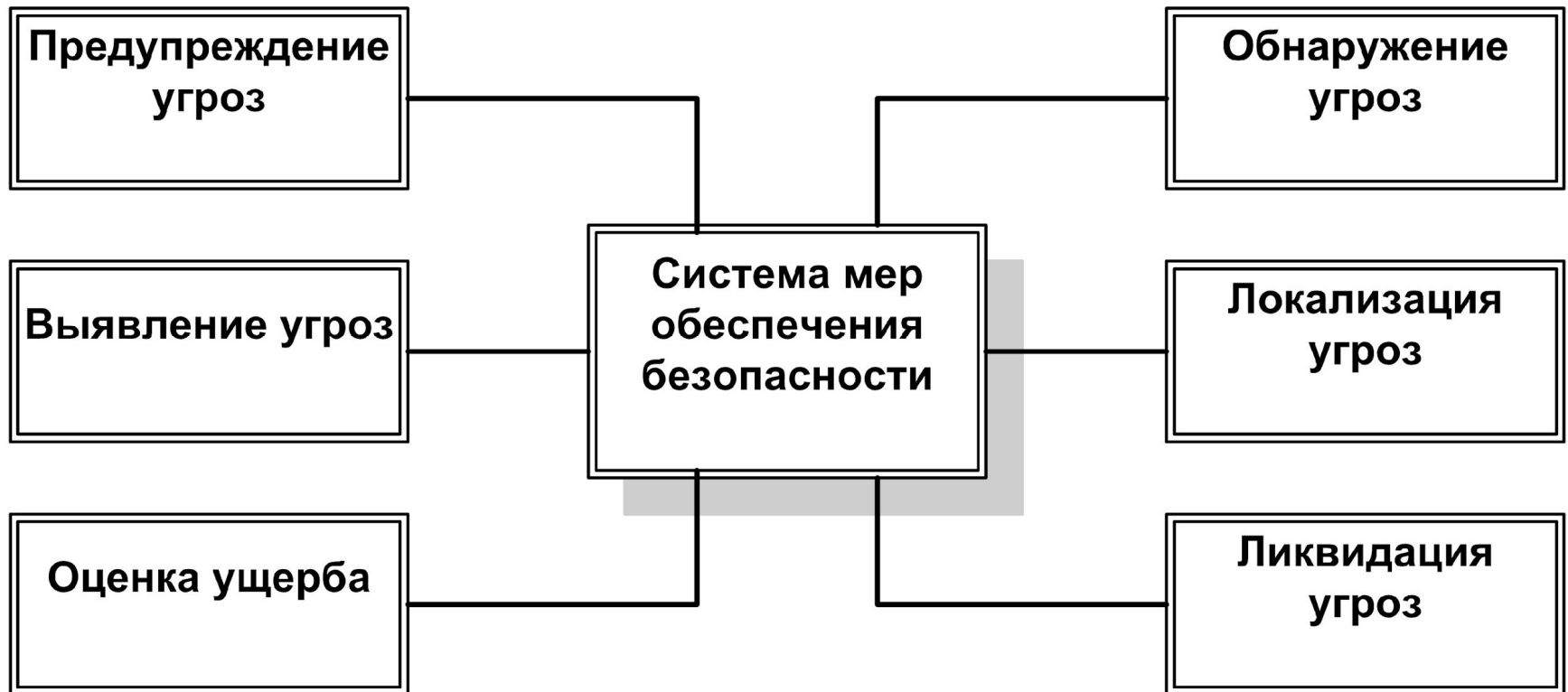
Зависимость прибыли предприятия от уровня риска.



Общая структура системы управления организацией.



Система обеспечения безопасности - комплекс мер по выявлению, предупреждению и пресечению внешних и внутренних угроз безопасности предприятия.



Содержание и сущность основных терминов и определений.

- Методика и методология безопасности?

- Объекты и субъекты безопасности?

- Границы исследования, где они?

Методологические подходы к обеспечению безопасности объектов.

Система «Волк и Красная шапочка»

**Снижение продолжительности негативного
воздействия на защищаемый объект.**

Снижение уязвимости объекта

- снижение восприимчивости объекта к различному роду негативных воздействий, т.е. снижение степени изменения его свойств под действием деструктивных факторов.
- В последнем случае принято говорить о *снижении уязвимости* объекта защиты, о которой упоминалось ранее.

Снижение вероятности возникновения того или иного негативного воздействия на защищаемый объект.

Аналитика – наше ВСЕ!

Снижение разнообразности возможных негативных воздействий (разновидности) на экономическую

Снижение силы негативного воздействия со стороны источника опасности на защищаемый объект.

- Своими силами.**
- Привлеченными силами.**

**Восстановление свойств защищаемого объекта
после оказанного на него негативного воздействия,
или замена поврежденного (уничтоженного) объекта
на аналогичный.**

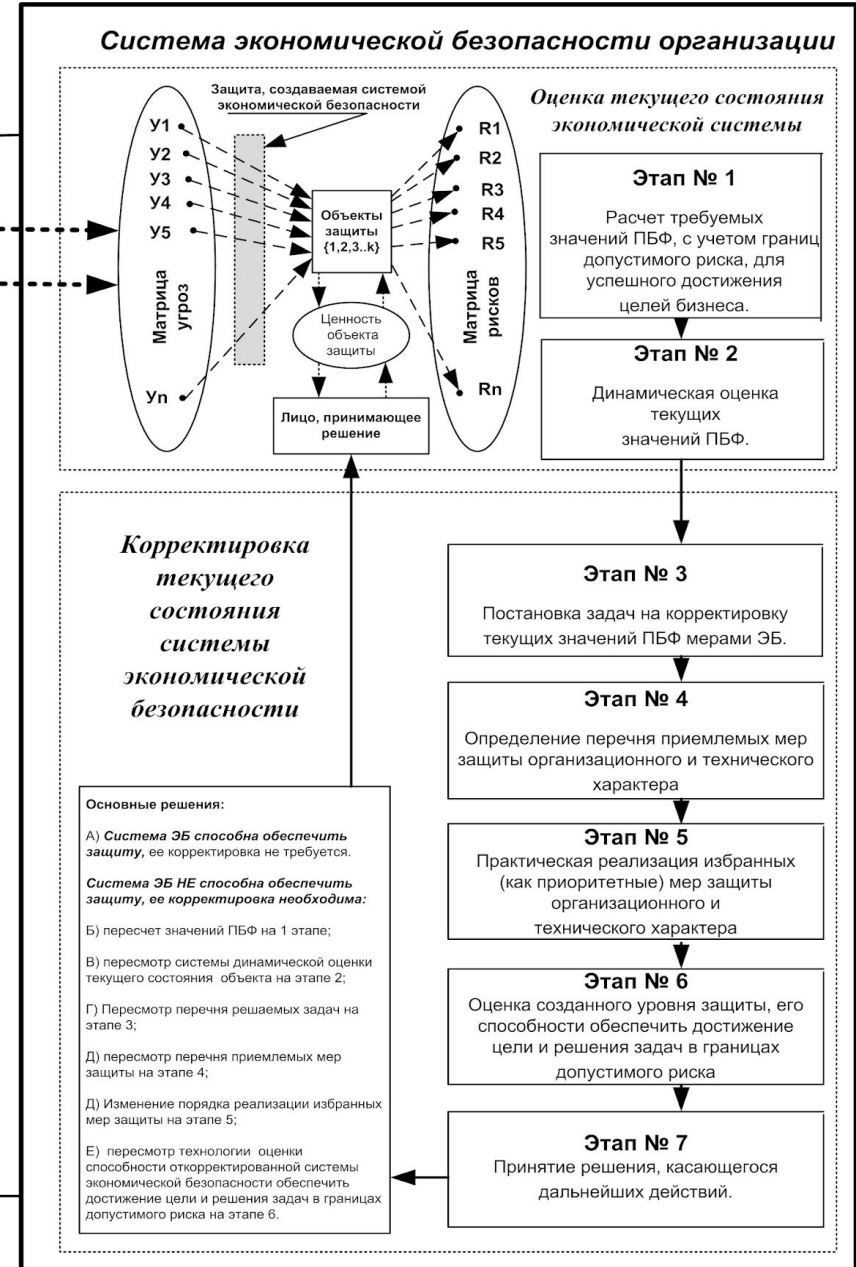
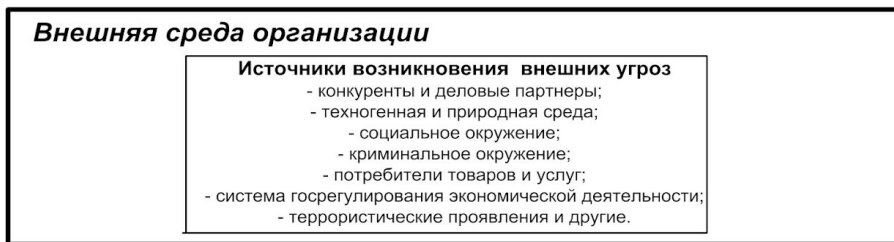
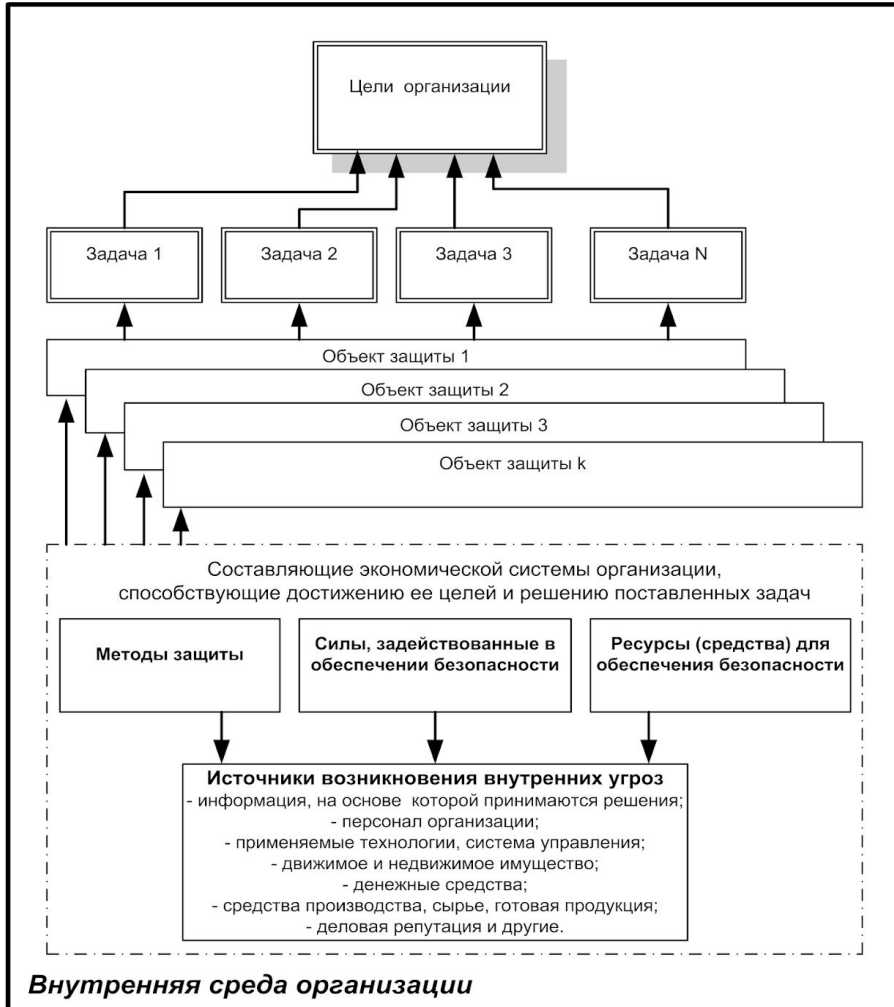


Методологические подходы к обеспечению безопасности объектов

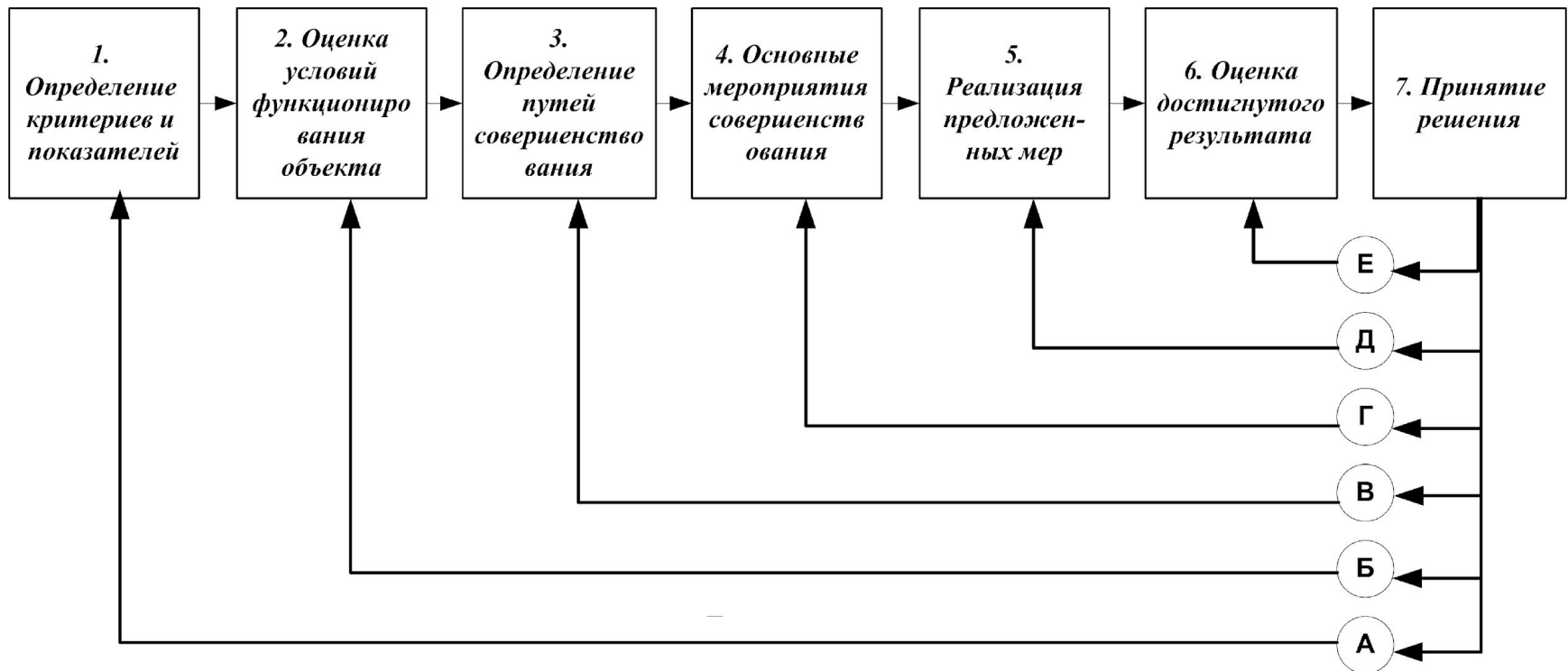
- **Во-первых**, на снижение продолжительности негативного воздействия на защищаемый объект.
- **Во-вторых**, снижение уязвимости объекта защиты, о которой упоминалось ранее.
- **В-третьих**, на снижение вероятности возникновения того или иного негативного воздействия на защищаемый объект.
- **В-четвертых**, на снижение разновидностей возможных негативных воздействий (разновидности) на экономическую систему.
- **В-пятых**, на снижение силы негативного воздействия со стороны источника опасности на защищаемый объект.
- **В-шестых**, на восстановление свойств защищаемого объекта после оказанного на него негативного воздействия, или компенсации нанесенного ущерба, например замены потерянного ресурса на аналогичный за счет «третьей стороны».

В зависимости от методологического подхода к обеспечению защиты объекта, выбранного как приоритетный, стоимость защитных мер будет различна!

Угрозы и риски. Взаимосвязь и взаимодействие.



Системный подход в обеспечении экономической и информационной безопасности субъектов хозяйственной деятельности.



Контрольно-проверочная деятельность, роль и место в системе безопасности объекта.

Методологические особенности и специфика системы управления информационным риском

- **Во-первых:** результат проявится не сразу.
- **Во-вторых:** сложность использования общепринятых рыночных механизмов ценообразования в связи с большой сложностью адаптации технологий защиты к специфике объекта.
- **В-третьих:** сложно увязать показатель уровня защиты с каким-либо конкретным решением
- **В-четвертых:** наличие желания персонала организации скрыть первопричины, истинные мотивы и факты нарушений политики безопасности, что существенно затрудняет оценку положительного эффекта от внедрения системы безопасности.
- **В-пятых:** комплексное воздействие отдельных мер защиты на экономическую деятельность организации, кроме положительного эффекта по одним параметрам может параллельно осуществлять и отрицательное воздействие

Особенности построение системы информационной безопасности в период экономического кризиса:

- изменение направлений деятельности СБ по необходимости;
- реорганизация СБ, исходя из снижения объема решаемых задач, в связи с передачей части функций на аутсорсинг;
- изменение концепции обеспечения безопасности предприятия;
- привлечение СБ к проведению антикризисных мероприятий;
- усиление мероприятий с увольняемыми сотрудниками с целью недопущения нанесения ими ущерба интересам предприятия после увольнения;
- увеличение количества и глубины внутренних расследований и проверок;
- увеличение количества мероприятий по пресечению противоправных действий со стороны персонала;
- увеличение количества мероприятий, направленной на вычисление ненадежных контрагентов;
- увеличение количества мероприятий, направленных на взыскание дебиторской задолженности.

Таким образом, для обеспечения требуемого уровня информационной безопасности защищаемого

объекта необходимо:

- **Во-первых**, стремиться реализовать одновременно несколько мер защиты, взаимодополняющих и не противоречащих друг другу. В тоже время, ни одна, даже очень крупная фирма, не может реализовать сразу все меры защиты, а те, которыми располагает, не может задействовать одновременно и в полном объеме.
- **Во-вторых**, эффективно использовать имеющиеся силы и средства обеспечения экономической безопасности. Особенно важно это обстоятельство для предприятий и организаций отраслей со сложными технологиями.

2. Подходы к экономической оценке целесообразности вложений в контрольно-проверочные мероприятия, зависит от ряда основополагающих факторов:

- **Наличия у предприятия средств, которые можно потратить на его СиБ.**
 - Средства неограниченны. (Требуется оценка стоимости проекта).
 - Средства имеют некоторые ограничение. (Что мы получим на сумму...?)
 - Средства жестко ограничены. (Решите нашу проблему...? Или пару- тройку самых важных проблем.)
- **Уровня компетентности руководителя в данном вопросе и его оценке проекта:**

Оценка проекта как ИНВЕСТИЦИОННОГО. (Ожидает возврат средств в виде прямой прибыли, чаще в виде предотвращенного ущерба, или повышения конкурентных преимуществ фирмы, позволяющих привлечь дополнительных клиентов, а значит и получить дополнительные прибыли).

Оценка проекта как ЗАТРАТНОГО. (Руководитель рассуждает с позиции: нам ничего не грозит, но пусть будет не хуже чем у конкурентов, или некуда деваться - требует Закон).

- Уровня компетентности специалистов по безопасности, выбирающих систему защиты более привычную для себя, отдавая предпочтения либо организационную, либо техническую подсистему. При этом ими в расчет принимается не более низкая стоимость системы, а более удобная и привычная для применения.
- Степень физической доступности средств защиты к защищаемому объекту.
- Временной фактор, т.е., может ли система безопасности быть создана и введена в эксплуатацию на защищаемом объекте в запланированные временные рамки.
- Наличие на объекте специалистов, способных решить поставленную задачу с заданным уровнем качества в установленное время.
- Наличие (отсутствие) нормативно-правовых ограничений (рекомендаций) на реализацию системы безопасности.
- Наличие технологий, способных решить задачу защиты объекта в данный момент времени, или требуется время и ресурсы для ее разработки и внедрения.

Основы «Экономики безопасности» В системе контрольно-ревизионной деятельности.

- Перейдя от методологии обеспечения экономической (информационной) безопасности в современных условиях к экономическим аспектам данной проблемы, рассмотрим основные подходы, касающиеся специфики финансирования контрольно-ревизионной деятельности в сфере обеспечения экономической безопасности (защиты информации).

Подход 1: СТОИМОСТНОЙ – применяется, в случае отсутствия особых ограничений в финансах, сводится к определению стоимости системы безопасности и обоснованию экономической целесообразности ее внедрения. При этом подходе возможны следующие варианты:

- **Применяются типовые решения** (стоимость которых известна) в области обеспечения безопасности по аналогии с другими подобными объектами. После их внедрения оценивается достигнутый уровень безопасности по ключевым показателям. В данном случае он обычно превышает оптимальный.
- **Проводится расчет показателей безопасного функционирования** объекта, после чего определяется перечень необходимых мероприятий, направленных на их достижение. Далее проводится расчет стоимости предложенных мероприятий и необходимого обеспечения для их реализации;

Подход 2: ЗАТРАТНЫЙ – применяется при строгой регламентации (ограничении) бюджета на создание системы безопасности.

В данном случае выделяются основные первоочередные угрозы и ведутся работы по их минимизации.

При этом некоторые из угроз так и остаются не локализованными.

Подход 3: КОМБИНИРОВАННЫЙ – применяется, чаще всего, на этапе становления бизнеса, в переходный период при расширении бизнеса или переходе предприятия в другие сферы деятельности.

В этом случае создается система безопасности включающая 2 составляющие:

- **постоянную**, позволяющую минимизировать несколько основных наиболее вероятных угроз, реализация которых наносит максимальный ущерб;
- **переменную**, позволяющую включать механизмы, минимизирующие последствия от реализации внезапно возникших деструктивных воздействий.

1. Результаты анализа различных подходов к созданию системы обеспечения безопасности ХС

Подходы в создании системы безопасности	Положительные аспекты	Отрицательные аспекты
<p>Стоимостной: Обычно применяется успешно развивающимися стабильно функционирующими предприятиями (банками), имеющими далеко идущие перспективы, совершенствующими свою систему безопасности накануне реализации ими новых программ, проектов, имеющие достаточные средства для развития.</p>	<ul style="list-style-type: none"> ● проект превентивно ориентированный, нацелен на предотвращение потенциального ущерба; ● проект нацелен на решение задач в комплексе; ● возможность планирования затрат и источников финансирования; ● возможность значительно варьировать базовыми показателями; ● достаточная система защиты ХС; ● возможность планирования и привлечения необходимого количества ресурсов; ● рассматривается чаще всего как инвестиционный проект; ● гарантии финансирования проекта и успешного его завершения; ● более качественное техническое и организационное обеспечение; ● возможность корректировки проекта, в процессе его реализации; 	<ul style="list-style-type: none"> ● большой расход средств на обеспечение безопасности; ● сложность расчета значений базовых показателей безопасного функционирования; ● отсутствие механизмов учитывающих корреляцию между отдельными показателями; ● сложность прогнозирования развития событий, их последствий и необходимых затрат; ● требуются более квалифицированные специалисты для реализации проекта;

2. Результаты анализа различных подходов к созданию системы обеспечения безопасности ХС

Подходы в создании системы безопасности	Положительные аспекты	Отрицательные аспекты
<p>Затратный Обычно применяется предприятиями с ограниченным финансированием, впервые создающим систему безопасности, планирующим резкое изменение деятельности, работающими по краткосрочным проектам, или одновременно в различных сферах деятельности.</p>	<ul style="list-style-type: none">• самые низкие, по сравнению с другими методами затраты на безопасность;• экономия средств на безопасность;• простота расчета и оценки;• малое время на реализацию.	<ul style="list-style-type: none">• проект изначально рассматривается как затратный, нацелен на создание минимально возможных условий безопасности объекта;• проект нацелен на решение только отдельных, наиболее важных задач, «латание дыр» в существующей системе безопасности;• сложность пересмотра и варьирования базовыми показателями;• ограниченность финансирования;• качество технического и организационного обеспечения ограничено бюджетом;• возможны перебои с финансированием

3. Результаты анализа различных подходов к созданию системы обеспечения безопасности ХС

Подходы в создании системы безопасности	Положительные аспекты	Отрицательные аспекты
<p>Комбинированный – применяется чаще всего на этапе становления бизнеса, в переходный период при расширении бизнеса, или смене предприятием сферы деятельности.</p>	<ul style="list-style-type: none">• меньшие расходы на систему безопасности по сравнению со стоимостным подходом;• создается более высокий уровень безопасности по сравнению с уровнем безопасности, созданном по затратному методу;• можно производить перераспределение бюджета в процессе создания, функционирования и совершенствования системы безопасности.	<ul style="list-style-type: none">• наличие «слабых мест» в существующей системе безопасности;• сложность прогнозирования времени, места реализации угроз, возможных последствий;• вероятность потерь от реализации угроз;• необходимость наличия резервов для компенсации возможного ущерба;• сложность управления системой безопасности.

Экономическая целесообразность системы защиты учитывается НЕ ВСЕГДА!

Фактическое завышение стоимости СЭБ связаны со следующими основными факторами (1):

- - создание системы безопасности, обеспечивающую избыточную защиту в текущий момент времени (Т), но экономически оптимальную для будущего момента времени (Тп), создающую предпосылки для успешного функционирования объекта в последующих временных интервалах его функционирования;
- - создание избыточной защиты по требованию нормативных актов (законов, Указов, распоряжений, инструкций, ГОСТов, СНИПов и т.д.);
- -создание системы безопасности для защиты государственной тайны;
- -создание избыточной защиты по требованию деловых партнеров, которые без выполнения их требований не готовы к сотрудничеству;
- -создание избыточной защиты по требованию вышестоящей (контролирующей, лицензионно-разрешительной, сертифицирующей и т.д.), организации;

Фактическое завышение стоимости контрольно-проверочных мероприятий связаны со следующими основными факторами (2)

- -принятие руководителем решения о применении более дорогой системы контроля в связи с использованием недостоверной (неполной, искаженной) информации о более дешевых системах (техничко-эксплуатационные показатели, сложности обслуживания, наработка на отказ и т.д.);
- - при выполнении требований по созданию делового имиджа, но отсутствии реальных угроз (ИКД ☺);
- -при отсутствии технологических (несовместимость старых и новых решений), организационных, временных, пространственных, природно-климатических и других возможностей применить более дешевые решения для проведения контрольно-проверочных мероприятий;
- -при принятии потребителем условий поставщика услуг (систем) контроля и оценки состояния объектов, проводящего агрессивную маркетинговую политику по распространению профильных систем;
- -в случае принятия решения под воздействием коррупционной составляющей (навязывание более дорогих решений);
- - приобретение контрольных систем с избыточными параметрами в связи с отсутствием опыта, в профильной сфере, что приводит к ошибкам в расчетах, переоценке угроз и т.д.;

Некоторые источники финансирования системы безопасности ХС в условиях ограниченности финансовых ресурсов.

- Создание условий безопасного функционирования ХС будет способствовать повышению их экономической эффективности, финансовой устойчивости, увеличению прибыли, не возможно без значительных финансовых вложений.
- Основным источником средств, направляемых на подобные проекты, являются чаще всего внутренние ресурсы предприятия, но возможно и привлечение средств и с внешних источников. На средства, выделяемые из госбюджета обычно рассчитывать не приходится.

Основными источниками финансирования, выделяющими средства на безопасность, обычно являются:

- **собственные финансовые средства** (прибыль, амортизационные отчисления, страховые возмещения, выплачиваемые страховыми компаниями, проценты по акциям, и т.д.);
- **средства от продажи основных фондов** (недвижимость, земля, имущество, транспорт и т.д.);
- **средства, полученные от продажи акций**, благотворительные и иные взносы, средства, выделяемые финансово-промышленными группами (ФПГ) на безвозмездной основе, иные взносы;
- **ассигнования из федерального бюджета**, бюджетов субъектов федерации, местных бюджетов;
- **иностранные инвестиции**, представленные в форме финансового или иного участия в уставном капитале совместных предприятий, а так же в форме прямых денежных вложений международных организаций и финансовых институтов, государств, предприятий различных форм собственности, частных лиц;
- **различные формы заемных средств**, в том числе кредиты, предоставляемые государством на возмездной основе, кредиты иностранных инвесторов, облигационные займы, векселя, кредиты банков и других институциональных инвесторов.

- **Спасибо за внимание!**