

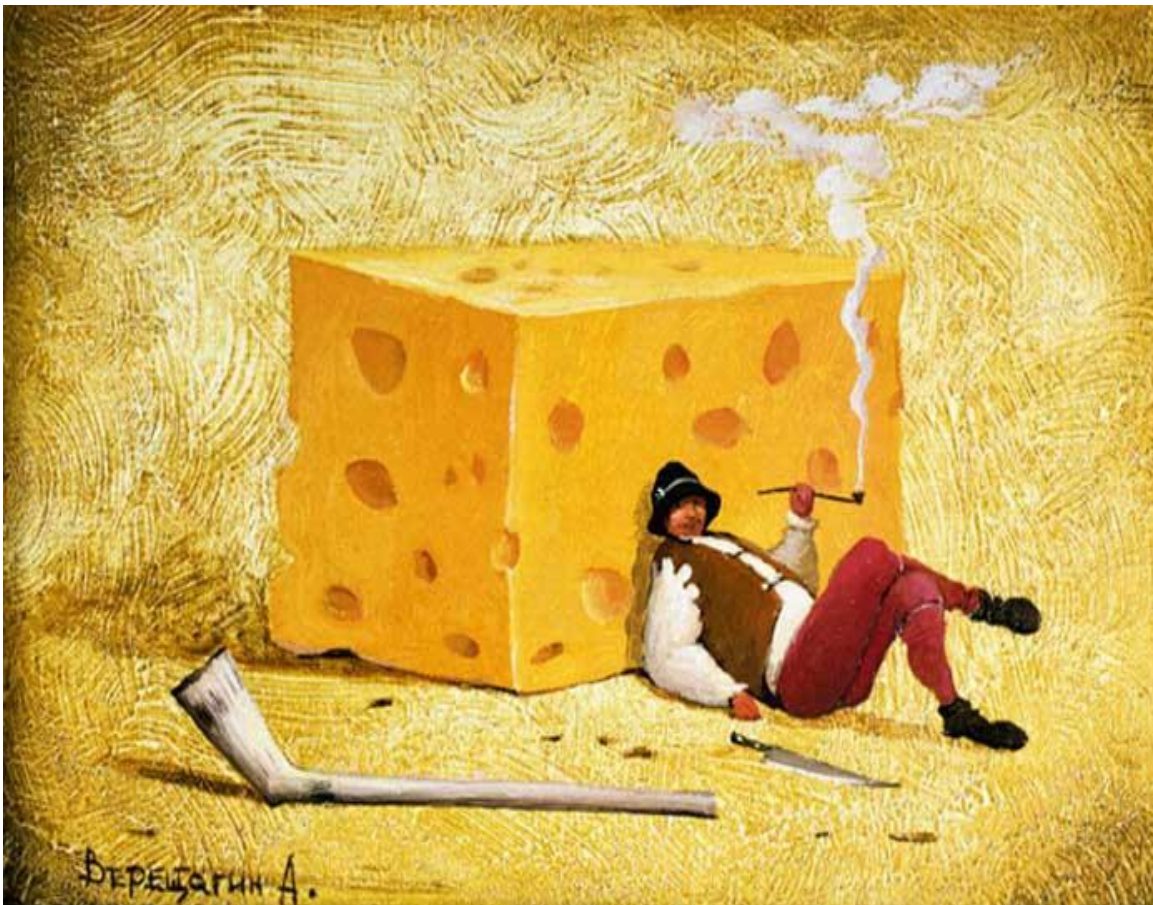
**Интересы личности, общества и государства в
динамике преодоления рисков и угроз безопасности**

Тема № 21



**Методология
организационного поведения.
Принцип
декомпозиции
системы «угроза-
защита»**

Лекция, 2 часа

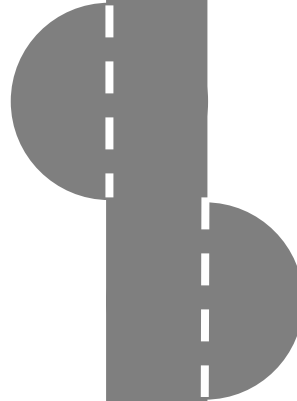




Разминка перед занятием: **прикладная конфликтология**



А



© fotolia

Б



- 1) Дорога однополосная;
- 2) С обеих сторон есть разъезды;
- 3) Преимуществ ни у кого нет;
- 4) Предположите возможные действия сторон;
- 5) Попробуйте описать структуру конфликта.



План лекции:

- 1. Функции системы безопасности бизнеса**
- 2. Построение системы мер**
 - Общий анализ рисков и угроз.
 - Построение защитных мер.
- 3. Принцип декомпозиции угроз и соответствующих им защитных мер**
 - Выделение угрозы.
 - Определение объекта защиты, его структурирование и классификация.
 - Определение возможных мер по реализации угрозы.
 - Построение системы защитных мер.
- 4. Расчет сил, средств и бюджета**
 - Численность требуемого персонала.
 - Инженерно-техническое оснащение.
 - Организационное построение и функционирование системы.
 - Мониторинг угроз.

Функции системы безопасности

Функции безопасности предприятия

Функции внутреннего аудита

Внутренний аудит

Финансовый мониторинг

Функции внешнего аудита

Функции службы безопасности

Экономическая безопасность

Финансовая безопасность

Кадровая безопасность

Информационная безопасность

Физическая безопасность

*Инженерно-техническая
безопасность*

Функции других подразделений

Валютный контроль

Противодействие коррупции

Автоматизация

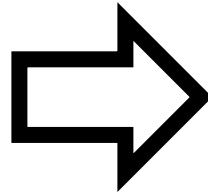
Промышленная безопасность



Относимость функций безопасности к компетенции различных подразделений

Наш бизнес

Его система
безопасности



Помимо рисков и угроз
внешней среды

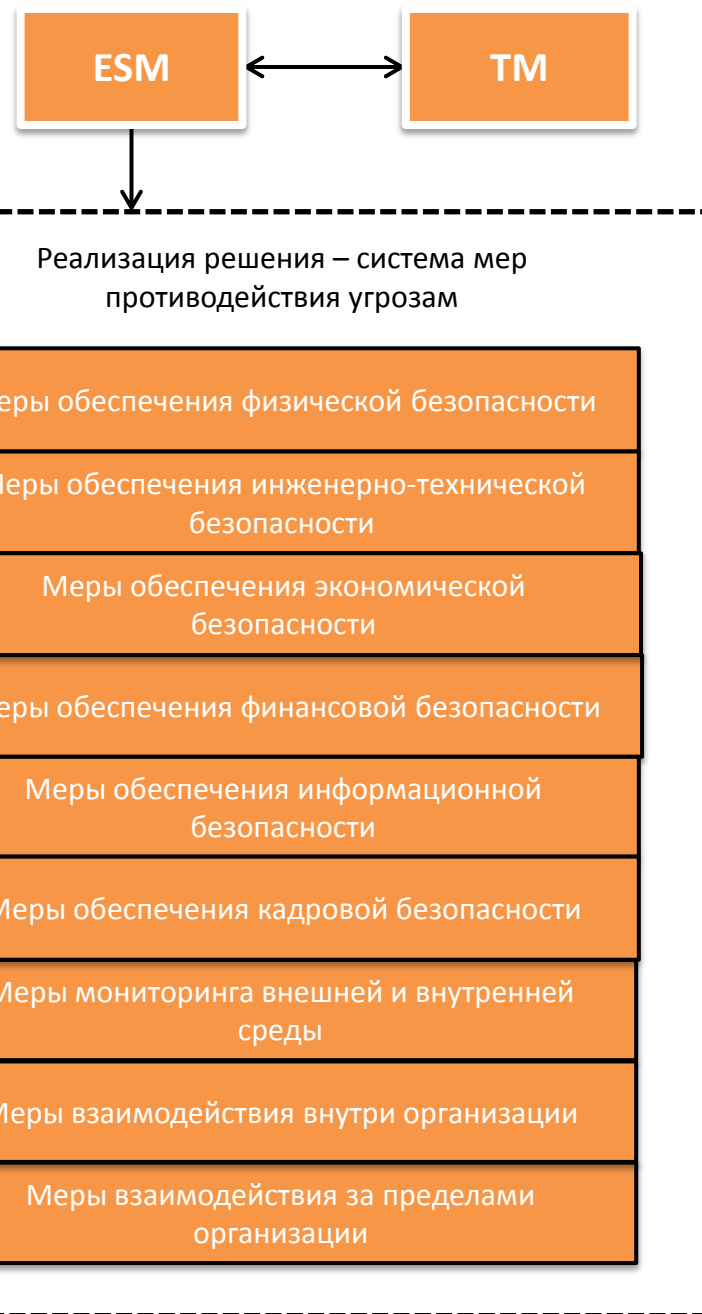
Анализ опыта успешных
участников рынка
(как они сумели минимизировать
угрозы?)

Анализ опыта покинувших рынок
участников
(что их погубило?)

Построение системы мер



Стадия построения системы мер



Угроза разглашения охраняемых сведений

Угроза жизни и здоровью работников

Угроза захвата собственности

Угроза хищения материальных ценностей

Угроза выбора несостоятельных контрагентов

Угроза внешнего и внутреннего мошенничества

Угроза промышленного шпионажа

Угроза нарушения стабильности электронных ресурсов

Угроза проникновения в персонал нежелательных лиц

ТЕОРИЯ И ПРАКТИКА ИСПОЛЬЗОВАНИЯ ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ СРЕДСТВ



1. Система контроля и управления доступом
2. Внешние устройства охранной сигнализации
3. Внутренние устройства охранной сигнализации
4. Противопожарная сигнализация
5. Устройства подачи тревожных сигналов
6. Внешние устройства видео наблюдения
7. Внутренние устройства видео наблюдения
8. Инженерная защита выделенных зон
9. Активная и пассивная защита от несанкционированного съема информации техническими средствами
10. Спутниковая навигация и связь
11. Система радиальной связи
12. Бронированные средства передвижения
13. Беспилотные летательные аппараты
14. Системы комплексного мониторинга
15. Система выявления взрывчатых веществ
16. Система поиска лиц по заданным параметрам

«Принцип стакана» – применим в любой сфере безопасности

Принцип декомпозиции

Стадия декомпозиции угрозы

Пример

ESM

1 – Виды охраняемых сведений

Угроза утечки охраняемых сведений

TM

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

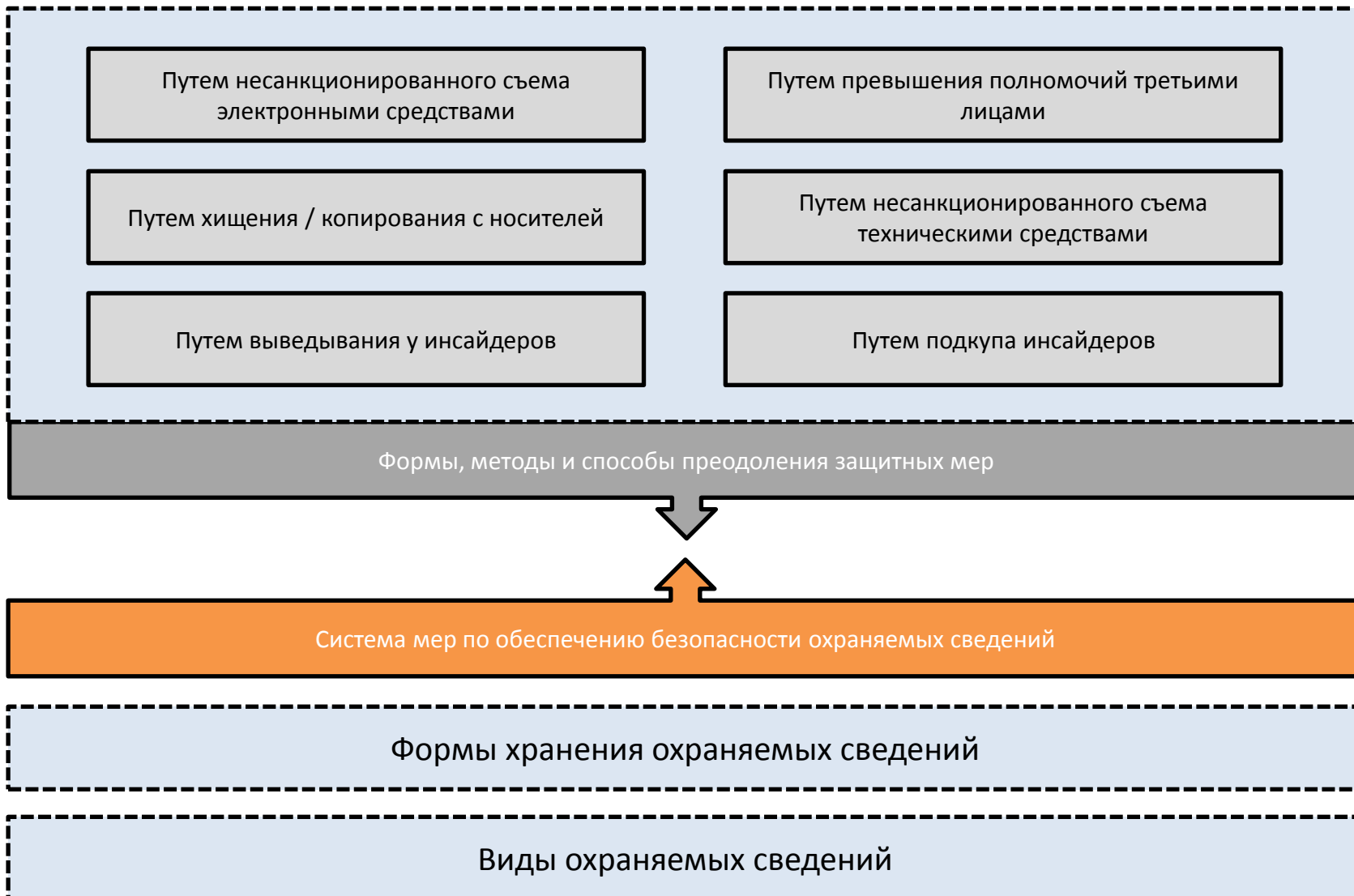
Менеджмент систем безопасности

Пример декомпозиции угроз:

4 – меры преодоления защиты

ESM

TM



Менеджмент систем безопасности

Пример декомпозиции защиты:

5 – меры упреждения ущерба

ESM

TM

Путем несанкционированного съема
электронными средствами

Меры защиты от несанкционированного съема
информации электронными средствами

Путем хищения / копирования с носителей

Меры защиты от несанкционированного проникновения в
места хранения защищаемой информации

Путем выведывания у инсайдеров

Меры правового закрепления ответственности,
повышения бдительности и мониторинга

Путем превышения полномочий третьими
лицами

Меры по своевременному получения данных о признаках
превышения полномочий

Путем несанкционированного съема
техническими средствами

Меры защиты от несанкционированного съема
информации техническими средствами

Путем подкупа инсайдеров

Меры мотивации персонала и закрепления правовой
ответственности за разглашение



Менеджмент систем безопасности

Оппоненты и защитники:

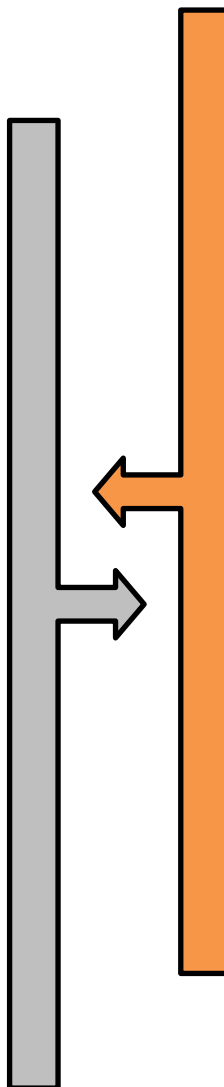
6 – понимание обстановки, расчет сил и средств



Средства радиоэлектронной и технической разведки



Зарубежные спецслужбы, конкуренты, отдельные преступники и преступные организации



ESM

TM



Служба безопасности предприятия и трудовой коллектив



Отечественные спецслужбы, частная охрана, правоохранительные органы, войсковая охрана и экстренные службы

Расчет сил, средств и бюджета



Рубеж контроля промышленной (ядерной) безопасности

Рубеж пропускного и внутри
объектового режима

Рубеж противодействия средствам
электронного и технического
проникновения, мониторинга персонала,
контрагентов и окружения объекта

6



5



4



Рубеж противодиверсионного и
антитеррористического
противодействия спецназа ФСБ РФ

3



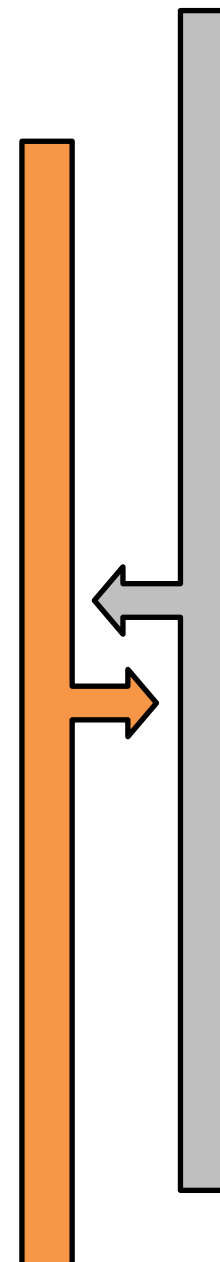
2



Рубеж войсковой охраны
внутренних войск МВД РФ

Средства инженерно-
технической защиты

1





Местные
спецслужбы



Российские дипломаты



Местные
специалисты



Защита персонала



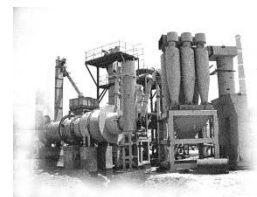
Группа
российских
специалистов



Местные
криминальные
группировки



Местная полиция и экстренные службы



Промышленный
объект

Зарубежное государство

Место
проживания,
объекты
посещения

Основные подходы к проблеме



Чем меньше охраняемых входов на объект, тем меньше требуется персонала охраны. Чем меньше персонала охраны, тем меньше фонд оплаты труда.



Один вооруженный охранник всегда стоит дороже одного охранника без оружия



Один односменный пост стоит дешевле поста круглосуточного



Инженерно-технические средства безопасности в определенный период обходятся дешевле, чем персонал охраны



Инженерно-технические средства безопасности не могут в большинстве случаев работать без участия персонала



Организация противодействия угрозам



С академической точки зрения...

- Эффективное противодействие угрозам предпринимательской деятельности возможно только в том случае, когда потенциальные угрозы известны, ранжированы и понятны по своим основным параметрам.
- При этом должен быть налажен их мониторинг в целях своевременного получения и оценки информации о том, что какая-либо угроза подошла к определенному критическому состоянию, когда она способна нанести реальный ущерб.
- Нельзя одновременно организовать действенный мониторинг всех перечисленных в данной теме потенциальных рисков и угроз. Из их числа каждое предприятие должно выделить ключевые угрозы.
- В отдельных случаях, возможно, придется принять разовые меры по недопущению или минимизации угроз. В других – нужна будет определенная постоянно действующая система мер, которая влечет за собой определенные затраты.
- Нормальный предприниматель не получает средств даром, по этой причине он всегда находится в дуалистическом состоянии: «Насколько реальна угроза и не превышен ли лимит средств на ее устранение?»
- О том, как эффективно организовать противодействие реально существующим угрозам пойдет речь в следующей теме.

Список электронных источников:

www.prmia.org – Международная ассоциация профессиональных риск-менеджеров (PRMIA)



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.

Принципы построения системы безопасности



С академической точки зрения:

- ☐ Построение системы безопасности не может основываться на абстрактных умозаключениях
- ☐ Система защиты всегда строится от реально существующих и потенциальных угроз
- ☐ Система безопасности не должна быть избыточной
- ☐ Система безопасности не должна быть недостаточной
- ☐ Система безопасности не может быть созданной однажды и на все времена
- ☐ Система безопасности должна быть оптимальной, всегда актуальной и динамичной
- ☐ Система безопасности должна быть высоко профессиональной
- ☐ Система безопасности должна быть нацеленной на постоянное совершенствование
- ☐ Система безопасности должна быть понятной топ-менеджменту предприятия и менеджерам взаимодействующих подразделений
- ☐ Система безопасности должна знать своих внутренних и внешних клиентов и работать с ними на стабильной основе
- ☐ Система безопасности должна соответствовать внутренней корпоративной культуре

Современный предприниматель должен понимать, что функция обеспечения безопасности является одной из составляющих общего управления бизнесом. Ее нельзя игнорировать в силу уже описанного джентельменского набора внутренних и внешних угроз.

По этой причине построение системы безопасности конкретного предприятия (группы компаний, холдинга) должно состоять из последовательных стадий:

- ❖ Прежде всего, должен быть проведен анализ внешней среды предприятия,
- ❖ должны быть определены общие и отраслевые риски,
- ❖ выделены ключевые угрозы.
- ❖ Анализ внутренней среды бизнеса также должен вскрыть основные проблемы.
- ❖ Всегда полезно в подобных случаях изучить ошибки и упущения тех предпринимателей, которые в данном секторе экономики потерпели поражение и вынуждены были свернуть свою деятельность.
- ❖ Такая комплексная аналитическая работа должна построить систему основных угроз, на пути которых следует построить защиту.

Практика уверенно свидетельствует о том, что построение систем безопасности не может основываться на абстрактных умозаключениях. Система защиты всегда строится от реальных угроз. При этом безопасность не может быть избыточной или недостаточной, созданной однажды и на все времена. Напротив, она должна быть оптимальной, всегда актуальной и динамичной. Более того, она также должна быть высоко профессиональной, понятной топ-менеджменту предприятия и менеджерам взаимодействующих подразделений, нацеленной на постоянное совершенствование.

Внимание !



Если менеджеры систем безопасности поверили в свою непогрешимость и совершенство, закрылись от посторонних взглядов завесой секретности, успокоились и посвятили себя «выращиванию орхидей и аквариумных рыбок» - это значит, что такую систему следует незамедлительно подвергнуть аудиту и принять меры по ее спасению в интересах последующего спасения самого бизнеса. Такая безопасность уже не защищает бизнес, она защищает только субъективные интересы и самомнение своих лидеров.

Требования к системам 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