ФИЛОСОФИЯ ЗАЩИТЫ

Экономика безопасности предприятия

Практика организации и управления: методики и технологии

Часть 4

Начало статьи читайте в № 01 (январь), 02 (февраль), 03 (март) 2014 г.

Данная статья посвящается 15-летию кафедры «Анализ рисков и экономической безопасности» Финансового университета при Правительстве Российской Федерации

ИНТЕГРИРОВАННАЯ СИСТЕМА БЕЗОПАСНОСТИ И ЕЕ ХАРАКТЕРИСТИКА. Оценка структуры затрат на создание и эксплуатацию инженерно-технической подсистемы системы безопасности.

Понятие интегрированной системы безопасности и ее характеристика

Сложность решения организационных и экономических задач обеспечения безопасности ХС обусловлена комплексным характером его функционирования, основными аспектами которого являются производственно-хозяйственная и финансовая деятельность. Следовательно, решение задач обеспечения безопасности, как мы рассмотрели выше, должно быть комплексным и основываться на функционировании системы обеспечения безопасности, в состав которой входит:

- интегрированная инженерно-техническая система безопасности (ИТСБ);
- интегрированная организационная составляющая системы безопасности (ИОТС).

Указанные выше подсистемы, их состав, структура, экономические особенности создания и функционирования будут рассмотрены ниже.

Особенность построения ИТСБ состоит в том, что одни и теже устройства одновременно решают разнородные задачи в интересах различных подсистем защиты. Например, видеокамера, управляемая специальным программным обеспечением (ПО), может одновременно работать в интересах системы видеонаблюдения, системе пожаровзрывобезопасности, системе контроля управления доступом (СКУД) и в других. В неинтегрированной системе в интересах каждой из отдельных подсистем работают свои устройства (часто аналогичные), локально решающие задачи в интересах отдельных подсистем защиты и не связанные друг с другом.

Таким образом, с одной стороны, интегрированные решения во внедряемой системе экономической безопасности повышают стабильность функционирования ХС, что не может не повлиять на положительную динамику роста его показателей, с другой стороны – являются весьма затратными, часто обременительными для ХС экономически.

Как было отмечено выше, одним из принципов обеспечения безопасности является разумная достаточность, определить которую можно с помощью методов и инструментов, позволяющих оценить величину затрат, планируемых руководством ХС

МИХАИЛ ВЛАСЕНКО,
доцент кафедры «Анализ рисков и экономическая безопасность»
Финансового университета при Правительстве РФ, кандидат экономических наук

для обеспечения безопасности своего бизнеса, по сравнению с тем эффектом, на который можно рассчитывать. Данный аспект будет рассмотрен в последующих публикациях.

Желательно данный фрагмент написать жирным шрифтом и убрать цветовое выделение.

Рассмотрим основные инженерно-технические подсистемы системы обеспечения безопасности (ИТСБ) ХС, их назначение и основные технические устройства, из которых они состоят, основные принципы расчета стоимости их внедрения, эксплуатации, технического обслуживания и ремонта.

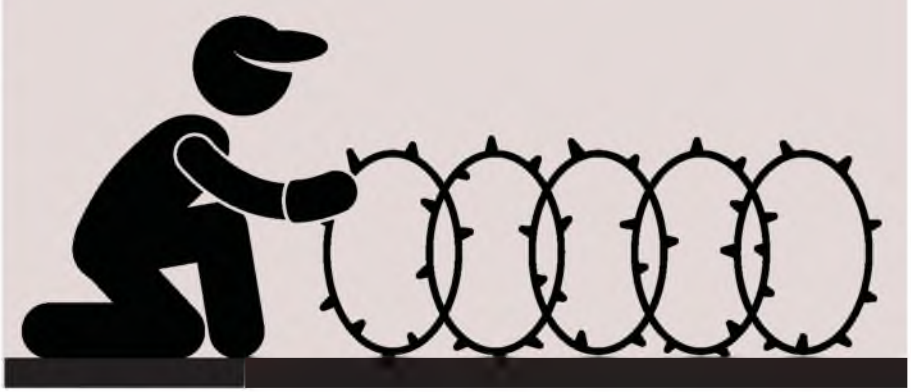
Выбирая те или иные устройства при проектировании инженерно-технических подсистем, учитываются следующие основные факторы, влияющие на итоговую (суммарную) стоимость будущих затрат, основными из которых являются:

- Политика ХС в отношении подхода к созданию системы обеспечения безопасности: стоимостной, затратный или комбинированный (о них мы говорили ранее).
- Политика ХС в отношении приоритетов использования брендов, производителей технических устройств и систем безопасности.
- Конечная цель внедрения системы обеспечения безопасности:

  - требует имидж предприятия;
  - требуют действующее законодательство, инвесторы, партнеры по бизнесу;
  - снижение явно определенных и неотвратимых потерь;
  - снижение явно неопределенных (потенциально возможных, вероятных) потерь, превентивные меры перед «рывком вперед», когда предприятие планирует развивать новые направления, выпускать новую продукцию, выходить на новые рынки;

- Наличие возможности выбора поставщиков системы безопасности в зоне временной и пространственной доступности.
- Наличие выбора и ассортимент систем безопасности, способных решить конкретную задачу в области защиты.

Одним из принципов обеспечения безопасности является разумная достаточность, определить которую можно с помощью различных методов и инструментов



- Степень понимания руководством предприятия необходимости внедрения той или иной системы безопасности, отдельных ее элементов и их возможности в конкретной обстановке, в данный момент времени.
- Уровень профессионализма сотрудников службы безопасности (СБ) в оценке целесообразности внедрения, экономической эффективности, функциональных возможностей предлагаемых систем, наличия навыков их эксплуатации.
- Наличия лимита времени на внедрение системы.
- Наличие реализованных на предприятии систем безопасности, возможности их наращивания и степени интеграции с новыми элементами предложенной системы.

Дадим краткую характеристику основным техническим подсистемам безопасности, рассмотрим их предназначение и состав.

А) Подсистема охранно-тревожной сигнализации и видеонаблюдения.

Назначение: обеспечение контроля состояния охраняемого объекта, своевременного обнаружения и оповещения о фактах несанкционированного проникновения злоумышленников на объект защиты или о их попытках совершить такие действия.

Технические устройства, входящие в состав:

- Управляющие, регистрирующие и приемно-контролирующие устройства;
- программное обеспечение;
- датчики (аналоговые, пороговые и др.), реагирующие на какие-либо из-

ТАБЛИЦА. СРАВНЕНИЕ СОСТАВА ОСНОВНЫХ ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ ПОДСИСТЕМ

Подсистема	А	Б	В	Г	Д
Управляющие, регистрирующие и приемно-контролирующие устройства	X	X	X	X	X
Программное обеспечение	X	X	X	X	X
Датчики	X	X	X		
Устройства фиксации и накопления данных	X	X	X	X	X
Устройства оповещения		X		X	
Устройства пожаротушения		X			
Идентификаторы			X	X	X
Ограждения			X		
Ворота, турникеты, шлюзы			X		
Запирающие и блокирующие устройства	X		X		
Носители информации о пользователе			X	X	X
Радиостанции			X	X	X
Устройства мобильной связи	X	X	X	X	X
Устройства интернет-телефонии	X	X	X	X	X
Устройства конференц-связи				X	
АТС			X	X	X
Устройства аудио видео трансляции и оповещения	X	X		X	
Периферийное сетевое оборудование	X	X	X	X	X
Локальная кабельная сеть	X	X	X	X	X
Устройства, обеспечивающие бесперебойное функционирование	X	X	X	X	X
Вспомогательное оборудование	X	X	X	X	X

менения или механические воздействия;
- устройства фиксации и накопления данных;
- устройства мобильной связи;
- устройства интернет-телефонии
- устройства оповещения;
- вспомогательное оборудование.

Б) Подсистема пожарной и взрывобезопасности.

Назначение: обнаружение фактов возгораний на охраняемом объекте, своевременное оповещение о них, осуществление локализации и ликвидации очагов возгорания.

Технические устройства, входящие в состав:
- управляющие, регистрирующие и приемно-контролирующие устройства;
- программное обеспечение;
- датчики (аналоговые, пороговые и др.), реагирующие на какие-либо изменения или механические воздействия;
- устройства фиксации и накопления данных;
- устройства оповещения;
- устройства пожаротушения;
- вспомогательное оборудование.

В) Подсистема контроля и управления доступом.

Назначение: регламентация доступа пользователей на объект, фиксация и протоколирование перемещений, исключающих неконтролируемое проникновение злоумышленника на охраняемую территорию (контролируемую зону).

Технические устройства, входящие в состав:
- управляющие электронные устройства;
- программное обеспечение;
- идентификаторы (механические, электрические, электронные, видео, биометрические и др.) и считыватели;
- датчики движения;
- устройства накопления данных;
- ограждения;
- ворота, турникеты, шлюзы;
- запирающие и блокирующие устройства;
- носители информации о пользователе: смарт-карты, электронные ключи и т. д.

Г) Подсистема связи и оповещения.

Назначение: передача и прием команд управления, оперативной информации о ситуации на объекте, оповещение лиц, находящихся на объекте.

Технические устройства, входящие в состав:
- управляющие электронные устройства;
- программное обеспечение;
- радиостанции (СВ, транкинговые, КВ, УКВ);
- системы мобильной связи;
- устройства пейджинговой связи;
- устройства интернет-телефонии;
- АТС;
- устройства конференц-связи;
- устройства аудио видео трансляции и оповещения;
- дополнительное и вспомогательное оборудование и т. д.

Д) Подсистема сбора, хранения, обработки, передачи и защиты данных.

Назначение: сбор, хранение, обработка, передача и защита, предотвращение утечки информации по техническим каналам, обеспечение аварийного восстановления утерянных сведений по причине технических сбоев и несанкционированного действия (НСД)пользователей.

57643@rambler.ru

Власенко Михаил Николаевич,
специалист в области безопасности бизнеса с более чем 20-летним стажем работы. Ранее находился на государственной службе. Стоял у истоков охранного бизнеса, руководил охранно-сыскным предприятием, службами безопасности инвестиционной компании, крупной торговой сети и Управляющей компании машиностроительного холдинга.
В настоящее время доцент кафедры «Анализ рисков и экономической безопасности» Финансового университета при Правительстве Российской Федерации, действующий эксперт Международной контртеррористической тренинговой ассоциации, независимый консультант по экономической безопасности, кандидат экономических наук. Разработчик множества эффективных методик защиты экономических интересов объектов, функционирующих в условиях рынка, автор ряда учебных курсов по безопасности бизнеса, написал более 50 работ по профильной тематике.

Технические устройства, входящие в состав:

- управляющие электронные устройства;
- программное обеспечение (система, почтовые программы, антивирусы, серверные программы, программы для работы в Интернете и т. д.);
- серверные устройства;
- локальная кабельная сеть, устройства и принадлежности для ее монтажа;
- периферийное сетевое оборудование (ХАБ, разветвители, коммуникаторы, кроссы, другое);
- устройства, обеспечивающие бесперебойное функционирование (устройства бесперебойного питания, климатическое оборудование, системы освещения, сигнализации, другие);
- дополнительное и вспомогательное оборудование, одноразовые инструменты и т. д.

Как видно из таблицы, представленной выше, большинство подсистем состоят из аналогичных технических устройств, которые в зависимости от поставленных задач могут выполнять те или иные функции в области обеспечения безопасности в интересах различных подсистем.

Большинство подсистем интегрированной системы безопасности состоят из конструктивно и функционально аналогичных технических устройств, которые могут решать различные задачи

При этом решаемые ими задачи могут изменяться с течением времени, функционал системы защиты и ее элементов остается тем же. Такой подход позволил создать интегрированные системы безопасности, отличающиеся многозадачностью, комплексностью, универсальностью, возможностями адаптироваться под изменение ситуации. Кроме того, данный подход позволяет упростить систему, оптимизировать ее структуру под задачи конкретной организации, минимизировать общие затраты на систему безопасности, поддерживать уровень безопасного функционирования ХС в рамках заданных показателей меньшими усилиями и ресурсными вложениями.

Стоимостная оценка подсистем инженерно-технической системы безопасности при ее создании и функционировании

В основе расчета стоимости реализации инженерно-технической составляющей интегрированной системы безопасности лежит оценка суммарных затрат на реализацию отдельных процедур и шагов (1).

$$C_З = \sum_{i=1}^{n} S_i , \qquad (1)$$

где:

$C_З$ – суммарная величина вложений в систему безопасности;

S_i – сумма вложений средств на реализацию i- й меры;

n – количество мер, направленных на повышение уровня безопасности объекта;

i – конкретная мера (действие, средство), способствующее повышению уровня безопасности объекта.

Рассмотрим более подробно содержание отдельных n-мероприятий в сфере безопасности (2).

$$\sum сз = \sum пп + \sum тс + \sum ук + \sum спп + \sum знп, \qquad (2)$$

где:

∑сз – суммарные затраты на реализацию ИТСБ;

∑пп – суммарная стоимость подготовки проекта внедрения ИТСБ;

∑тс – стоимость технической составляющей проекта;

∑ук – стоимость услуг контрагентов;

∑спп – суммарные расходы на содержание персонала своего предприятия;

∑знп – средства предприятия, потраченные на борьбу с ущербом, вызванным непреднамеренными потерями в процессе реализации проекта.

Расходы на подготовку проекта внедрения ИТСБ рассчитываются как суммарные затраты на выполнение ряда необходимых для этого мероприятий (3):

$$\sum пп = \sum ти + \sum а + \sum п + \sum ми + \sum т + \sum др, \qquad (3)$$

где:

∑пп – суммарная стоимость подготовки проекта внедрения ИТСБ;

∑ти – стоимость технологических исследований;

∑а – аудит состояния существующей системы безопасности;

∑п – планирование и подготовка мероприятий, направленных на создание ИСБ;

∑ми – изучение опыта обеспечения безопасности в аналогичных компаниях (маркетинговые исследования);

∑т – стоимость организации и проведения тендеров;

∑др – суммарная стоимость мероприятий деловой разведки (сбор, получение, обработка, анализ информации, подготовка отчетов).

Стоимость технической составляющей рассчитывается как суммарные затраты на закупку необходимых устройств, материалов и комплектующих, необходимых для осуществления монтажа (4).

В данном случае, в зависимости от вида закупаемой продукции, системы бухгалтерских проводок и действующей системы налогообложения, часть изделий может быть зачислена в разряд основных фондов, что приведет к дополнительным затратам в виде обязательных дополнительных налоговых и других выплат.

$$\sum тс=\sum ту+\sum рм+\sum км+\sum по, \quad (4)$$

где:

∑тс – стоимость технической составляющей проекта;

∑ту – суммарная стоимость технических устройств, изделий;

∑рм – суммарная стоимость расходных материалов;

∑км – суммарная стоимость комплектующих материалов;

∑по – суммарная стоимость программного обеспечения;

Стоимость услуг контрагентов, рассчитывается как суммарные затраты на работы, выполняемые сторонними организациями. (5):

$$\sum ук=\sum и+\sum эо+\sum к+\sum мо+\sum пнр+\sum ду, \quad (5)$$

где:

∑ук – стоимость услуг контрагентов;

∑и – суммарная стоимость исследований;

∑эо – суммарная стоимость экспертных оценок;

∑к – суммарная стоимость консультаций;

∑мо – суммарная стоимость монтажа оборудования;

∑пнр – суммарная стоимость пусконаладочных работ;

∑ду – суммарная стоимость транспортных и других услуг.

∑ндс – налог на добавленную стоимость.

Суммарные расходы на содержание персонала предприятия рассчитываются как сумма затрат на выдачу оклада, выплату надбавок, премий, материальной помощи, с учетом обратных вычетов в виде штрафов, налоговых и других удержаний и т. д. (6):

$$\sum спп=(\sum о+\sum нб+\sum пр+\sum мп+)-(\sum шт+\sum ду), \quad (6)$$

где:

∑спп – суммарные расходы на содержание персонала своего предприятия;

∑о – суммарный размер выплат по основному окладу;

∑нб – суммарный размер выплат по надбавкам;

∑пр – суммарный размер выплат по премиям;

∑мп – суммарный размер выплат по материальной помощи;

∑шт – суммарный размер удержаний по штрафам;

∑ду – суммарный размер других удержаний.

При планировании затрат, необходимых для реализации системы безопасности, необходимо учитывать множество факторов одновременно

Затраты предприятия от непреднамеренных потерь рассчитываются как сумма затрат на борьбу с ущербом, вызванным непреднамеренными потерями (7):

$$\sum знп=\sum бт+\sum тс+\sum оп+\sum па, \quad (7)$$

где:

∑знп – средства предприятия, потраченные на борьбу с ущербом, вызванным непреднамеренными потерями в процессе реализации проекта;

∑бт – суммарные потери от брака и нарушения технологии при реализации проекта;

∑тс – суммарные потери от технологических сбоев;

∑оп – суммарные потери от ошибок персонала в процессе монтажа системы, проведении пусконаладочных работ, эксплуатации, технического обслуживания и ремонта;

∑па – суммарные потери от поломки аппаратуры.

При планировании затрат, необходимых для реализации системы безопасности, необходимо учитывать следующие основные факторы:

- периодичность их возникновения (разовые и текущие);
- возможности охвата планированием (планируемые и непланируемые);
- зависимость от объема производства (постоянные и переменные).

Остальные признаки классификации затрат, рассмотренные нами в предыдущих публикациях, учитываются экономистами и бухгалтерами в соответствии с:

- принятой в организации учетной политикой;
- действующей системой налогообложения;
- системой финансирования проекта, и рядом другими.

Для лиц, принимающих решения в области безопасности, последняя группа факторов не представляет особого интереса, как не оказывающая существенного влияния на особенности финансирования и специфику реализации проекта.

Организационная составляющая системы экономической безопасности хозяйствующего субъекта, характеристика ее основных подсистем, оценка структуры затрат на ее создание и эксплуатацию будут подробно рассмотрены в последующих публикациях.

Продолжение следует