Затраты на обеспечение информационной безопасности предприятия

можно подразделить на *единовременные и систематические*

Единовременные затраты включают в себя:

1) Затраты на формирование звена управления системой защиты информации и другие организационные затраты;

2) Затрат на приобретение и установку средств защиты.

Систематические затраты включают в себя:

Затраты на обслуживание системы информационной безопасности:

- затраты на осуществление технической поддержки производственного персонала при внедрении средств защиты информации;
- затраты на организацию системы допуска исполнителей и сотрудников конфиденциального делопроизводства;
- затраты на обслуживание и настройку программно-технических средств защиты, операционных систем, сетевого оборудования;
- затраты на организацию безопасного использования информационных систем;
- затраты на обеспечение бесперебойной работы системы защиты информации.

Затраты на контроль работы системы безопасности:

- затраты на контроль изменений состояния информационной среды предприятия;
- затраты на контроль за действиями персонала;
- затраты на плановые проверки и испытания программно-технических средств защиты информации;
- затраты на проведение проверок навыков персонала предприятия по эксплуатации средств защиты;
- затраты на контроль правильности ввода данных в прикладные системы;
- оплата труда инспекторов по контролю требований, предъявляемых к защитным средствам, обеспечивающих управление защитой коммерческой тайны.

Затраты на обеспечение должного качества информационных технологий и их соответствия требованиям стандартов:

- затраты на обеспечение соответствия требованиям качества информационных технологий;
- затраты на обеспечение соответствия принятым стандартам и требованиям достоверности информации, действенности средств за-щиты;
- затраты на доставку и обмен конфиденциальной информации;
- затраты на удовлетворение субъективных требований пользователей: стиль, удобство интерфейсов.

Затраты на повышение квалификации персонала в вопросах использования имеющихся средств защиты, выявления и предотвращения угроз безопасности.

Затраты, связанные с пересмотром политики информационной безопасности предприятия:

- затраты на идентификацию угроз безопасности;
- затраты на поиск уязвимостей системы защиты информации;
- оплата работы специалистов, выполняющих работы по определению возможного ущерба и переоценке степени риска;
- затраты на внедрение дополнительных средств защиты информации.

Затраты на ликвидацию последствий нарушения режима информационной безопасности:

- затраты на **восстановление** системы безопасности до соответствия требованиям политики безопасности.
- затраты на **приобретение** новых технических средств;
- затраты на **утилизацию** пришедших в негодность ресурсов;
- затраты на **восстановление** баз данных и прочих информационных ресурсов;
- затраты на проведение мероприятий по **контролю** достоверности данных, подвергшихся атаке на целостность;
- затраты на проведение дополнительных испытаний и проверок информационных систем;
- затраты на проведение **расследований нарушений** политики безопасности;
- затраты на юридические споры и выплаты компенсаций;
- затраты, возникшие вследствие разрыва деловых отношений с партнерами.

Затраты, возникающие в результате потери новаторства:

- затраты на проведение дополнительных исследований и разработки новой рыночной стратегии для предприятия в связи с отказом от организационных, научно-технических, коммерческих решений, ставших неэффективными в результате утечки сведений;
- затраты, возникшие из-за снижение приоритета в научных исследованиях и невозможности патентования и продажи лицензий на научно-технические достижения.

Классификация затрат условна, так как детальная разработка перечня зависит от особенностей конкретной организации и ее систем защиты информационной безопасности.

Обычно неизбежные затраты, которые необходимо учитывать даже если уровень угроз безопасности достаточно низкий, включают в себя следующие статьи:

- обслуживание технических средств защиты;
- конфиденциальное делопроизводство;
- функционирование и аудит системы безопасности;
- минимальный уровень проверок и контроля с привлечением специализированных организаций;
- обучение персонала методам информационной безопасности.

При соблюдении политики безопасности и проведении профилактических мероприятий можно исключить или существенно снизить следующие затраты:

- на восстановление системы безопасности до соответствия требованиями политики безопасности;
- на восстановление ресурсов информационной среды предприятия;
- на переделки внутри системы безопасности;
- на юридические споры и выплаты компенсаций;
- на выявление причин нарушения политики безопасности.