ЭКОНОМИКА ЗАЩИТЫ ИНФОРМАЦИИ

Экономический подход к защите информации включает

1. Изучение вопросов экономической оценки информационных ресурсов.

2. Получение знаний о методах оценки угроз и степени риска в деятельности предприятия.

3. Знакомство с технико-экономическими задачами обеспечения информационной безопасности.

4. Формулирование и решение задач создания экономически обоснованных систем информационной безопасности (СИБ) предприятия.

Экономическая задача создания СИБ предприятия

Задача может формулироваться исходя из возможностей предприятия или заданной эффективности системы:

1. При заданном заданном объеме расходуемых ресурсов обеспечить достижение максимально возможного результата.
2. Обеспечить достижение заданного результата при минимальном расходовании необходимых ресурсов.

Экономическая оценка эффективности информационного обеспечения

Оценка экономической эффективности информационного обеспечения производится по двум составляющим:

1-**по экономии времени руководителей и специалистов, занятых подготовкой решений**;

2-**по экономии, обусловленной использованием полученных научно-технических материалов**.

За основу принимаются нормативные трудозатраты, с точки зрения потребителя информации.

Тогда, **экономию по первой составляющей за год** можно подсчитать по формуле:

Эt=0,545 (∆tд*Зср.д*Nд+∆tи*Зср.и*Nи), где

0,545 - отношение числа месяцев в году к среднему числу рабочих дней в месяце;

∆tд - экономия времени руководителей за счет информационного обеспечения (дней в месяц);

Зср.д - среднемесячная зарплата одного руководителя, обеспечиваемого информацией (руб.);

Nд - число руководителей, получивших информацию и принявших ее к использованию;

∆tи; Зср.и; Nи - то же для специалистов, обеспечиваемых информацией и принимающих участие в подготовке решений.

Экономию затрат на разработку и внедрение научно-технических достижений по информационным материалам **($Э_3$)** можно рассчитать по формуле

$$Э_3 = В_1 - (В_2 – В_Р),$$ где,

$В_1$ - затраты на разработку достижений при отсутствии информации (техдокументации);

$В_2$ - затраты на доработку достижений при их внедрении;

$В_Р$ - расходы на получение техдокументации.

Обозначим время, необходимое на собственную разработку новшества - $T_р$, тогда выигрыш во времени за счет использования материалов НТИ составит:

$$\tau = T_р - (T_в + t_{инф}),$$ где

$T_в$ - время внедрения новшеств;

$t_{инф}$ - время, затраченное на информационные процессы.

Годовой **экономический эффект от ускорения реализации экономического потенциала** новшеств определяется годовой экономией $Э_т = E_н * Э_п * \tau$, где

$E_н$ - нормативный коэффициент эффективности капитальных вложений;

$Э_п$ - потенциальный экономический эффект заложенный разработчиками.

Доля экономии, приходящейся на информационную службу **($Э_и$)**, определяется по формуле

$$Э_и = Э_н – З_и/З_{р.в},$$ где

$Э_н$ - годовая экономия от использования новых технических средств, созданных при участии службы НТИ;

$З_и$ - годовой фонд зарплаты штатных и внештатных сотрудников информационной службы;

$З_{р.в}$ - годовой фонд зарплаты специалистов, занятых разработкой и внедрением новшеств.

Тогда **суммарный годовой эффект** информационного обеспечения **($Э_{нти}$)** с учетом составляющих экономии, рассмотренных выше, определяется как

$$Э_{нти} = Э_t + Э_з + Э_т + Э_и - (С_{нти} + Е_н * К_{нти}),$$ где

$С_{нти}$ - себестоимость информационных работ, включающая текущие затраты на их проведение;

$К_{нти}$ - капитальные вложения в информационную систему.

Эффект от использования информационных материалов на различных этапах жизненного цикла технических новшеств состоит:

в экономии затрат на разработку и внедрение новой техники,
в сокращении сроков разработки, освоения и модернизации технических средств и технологических процессов,
в росте производительности труда руководителей и специалистов.

Коэффициент эффективности использования информационных материалов можно определить по формуле:

Кэ= Эо/Зи, где

Эо – общая экономия производственных затрат за счет информационной деятельности;

Зи – общие затраты на информационную работу.

Защита ОИС в предпринимательской деятельности

Объектами интеллектуальной собственности (ОИС) **являются результаты интеллектуальной деятельности** и средства индивидуализации труда участников предпринимательской деятельности.

Главный критерий при отнесении таких объектов к ОИС - **наличие правовой охраны**, что означает признание исключительных прав правообладателя на такой объект.

Охранно-способными результатами интеллектуальной деятельности (в соответствии с ГК РФ) **являются :**

произведения науки, литературы и искусства, а также другие объекты авторских и смежных прав;

- **изобретения**, полезные модели, промышленные образцы;
- **программы для ЭВМ** и базы данных;
- **топология интегральных микросхем**;
- **селекционные достижения**;
- **секреты производства (ноу-хау)** - техническая организационная или коммерческая информация, защищается как КТ от незаконного использования третьими лицами.

Для целей бизнеса и оценки, связанной с этим целями, различают три вида ноу-хау:

1. **Неотделимые от конкретного индивидуума** (физического лица), в том числе индивидуальные навыки и умения.
2. **Неотделимые от конкретного предприятия** (юридического лица) технологии, основанные на традиции или предполагающие необычно высокую культуру производства.
3. **Отделимые в общем случае от предприятия или индивидуума**, в том числе: сознательно скрываемые технические сведения, рисунки, чертежи, а также «условные» (номинальные) ноу-хау, т.е. сохраняемые в секрете патентно-способные результаты.

Оценка рыночной стоимости (Ци) объекта ИС производиться по формуле:

$Ц_и = [(С_р + С_п + С_м)*К1*К2*К3*К4 + р*Ar*Т]*К5*К6$, где:

$С_р$ – приведенные (к одному временному периоду) затраты на создание объекта;
$С_п$ – приведенные затраты на обеспечение правовой охраны объекта;
$С_м$ – приведенные затраты на маркетинговые исследования;
р – среднестатистическая ставка роялти (лицензионных выплат);
Ar – база для расчета роялти годовой объем использования;
Т – срок полезного использования ОИС;
К1 – коэффициент технико-экономической значимости объекта ;
К2 – коэффициент промышленной готовности объекта правовой охраны;
К3 – коэффициент надежности правовой охраны оцениваемого объекта;
К4 – коэффициент морального старения оцениваемого объекта;
К5 – коэффициент амортизации стоимости оцениваемого объекта на момент расчета;
К6 – коэффициент правовой значимости оцениваемого объекта интеллектуальной собственности.

Данная формула может быть использована для расчета рыночной цены объекта ИС, например, для целей продажи лицензии, внесения долевого пая в уставной капитал предприятия и др.

Итоговая стоимостная оценка объекта ИС при расчете его рыночной цены может быть скорректирована по договору между его субъектами (сторонами).

В этом случае бонификация (надбавка) к стоимостной оценке объекта с учетом факта риска не должна превышать 30% его расчетной рыночной стоимости.

Литература. Н. Лынник. Международные стандарты оценки и сертификации стоимости объектов ИС. // Интеллектуальная собственность №9-10, 1996.

Персонал фирмы и его роль в утечке информации

Анализ угроз информации позволил выделить следующие виды угроз информационным ресурсам - по степени их опасности:

-некомпетентные служащие; - (30%)
-хакеры и крэкеры; - (4%)
-неудовлетворенные своим статусом служащие;
-нечестные служащие; - (60%)
-инициативный шпионаж;
-организованная преступность;
-политические диссиденты; - (6%)
-террористические группы.

Психологические приемы добывания коммерческой информации

Можно выделить два основных способа добывания интересующей нас информации.

Первый – это побуждение субъекта к непроизвольным высказываниям фактов, представляющих интерес для сотрудника службы разведки фирмы.

Второй – побуждение субъекта к непроизвольным физическим или экспрессивным действиям, содержащим соответствующую, интересующую фирму информацию.

Основные приемы добывания информации

Демонстрация конкретных предметов.

Использование смежной темы разговора.

Использование тщеславия и честолюбия.

Проявление равнодушия.

"Игра" на чувстве собственного достоинства

Проявление участия.

Принципы профотбора персонала

1.Применение психологических подходов к профотбору
(с использованием **тестовых методик**)

-выявление ранее имевших место судимостей, преступных связей, криминальных наклонностей;

-выявление предрасположенности кандидата к совершению противоправных действий, дерзких и необдуманных поступков при формирования в его окружении в определенных обстоятельств;

-установление фактов, свидетельствующих о морально-психологической неустойчивости кандидата на работу.

2.Использование организационных схем управления и профессиограмм

Оргсхемы (чертежи на которых графически изображается каждое рабочее место, для которых прописываются должностные обязанности и определяются информационные потоки).

Профессиограммы (профиль требований), перечень личных качеств, которыми должен обладать потенциальный сотрудник.

Для **дополнительного анализа** анкеты кандидата и его фотографий приглашаются **юристы**, **графологи**, **психоаналитики** и даже **экстрасенсы** с целью обеспечения максимальной **точности заключения** и **выявления возможных скрытых противоречий** в характере проверяемого лица.

В последние годы широко практикуется **почерковедческая экспертиза**, которая позволяет определить:

темперамент, выдержку, волевые качества, собранность, аккуратность, грамотность, общеобразовательный уровень и пр., а также предрасположенность кандидата к совершению неблаговидных и нечестных поступков.

Тестовые методики подразделяются на четыре группы:

- **Личностные опросные листы (тесты):** СМИЛ, КЕТТЕЛА, MMPI, АЗЕНКА, РСК, КУ-СОРТ, ТОМАСА, УСК
- **Бланковые методики:** тесты РАВЕНА, ВЕКСЛЕРА, АМТХАЭРА, методика компасов, таблица ШУЛЬЦА и другие.
- **Проективные методики:** цветовой тест ЛЮШЕРА, пятна РОРХАНА, тест РОЗЕНЦВЕЙГА.
- **Приборные методики:** использование ПОЛИГРАФА и др. приборов.

Основные этапы профотбора

Первый этап. Предварительное собеседование.

Второй этап. Сбор и оценка информации о кандидатах.

Третий этап. Тестовые приемы проверки кандидатов.

Четвертый этап. Исследование результатов тестирований.

Пятый этап. Заключительное собеседование. На заклчительном этапе следует обращать особое внимание на соответствие поведения кандидата своему типу темперамента.

Планирование действий в чрезвычайных ситуациях

Условием быстрого преодоления чрезвычайных ситуаций является **разработка планов** обеспечения бесперебойной деятельности компании, восстановления и резервирования информации и восстановления деятельности.

Для преодоления ЧС на предприятии **создается кризисная группа,** состоящая из ответственных лиц.

В плане указываются следующие сведения:

-имена, адреса и номера телефонов ведущих сотрудников;
-цели и обязанности сотрудников при ЧС;
-списки необходимых ресурсов, включая технические средства, программное обеспечение, средства связи, документы, и персонал;
-вспомогательная информация (маршруты перевозок, карты, адреса, и т.д.);
-схемы мобилизации персонала и восстановительных работ;
-административная координации работ, связанных с восстановлением;
-список адресов для рассылки плана действий в ЧС;
-процедуры постоянной корректировки и испытаний плана.

Следует ежеквартально проводить проверку плана, поддерживая точность сведений о координатах ведущих сотрудников.

Испытания плана проводятся в **два этапа**:

-сначала **анализируется каждый элемент плана**,
-затем **имитируется бедствие для реализации схемы действий** в полном объеме.

Оценка затрат на планирование мероприятий.

Применительно к банковской деятельности затраты на планирование **не должны превышать 1%** общих затрат на обработку данных.

Анализ и оценка риска

Методы анализа риска:

-статистический;
-аналитический;
-экспертных оценок;
-аналогий.

Степень риска $К_р = У_{max} / С$; где:

$У_{max}$ – максимально возможная сумма убытков [руб.];

С – объем собственных ресурсов [руб.].

Ожидаемые потери при реализации угрозы рассчитываются по следующей **формуле:**

$$E = V \cdot p, \text{ где } V = S \cdot (1 - Кз),$$

p – вероятность возникновения угрозы;

V – оценка ущерба при реализации угрозы;

Кз – коэффициент защищенности системы информационной безопасности ;

S – стоимость актива.

Способы минимизации риска

Избежание риска означает уклонение от мероприятий, связанных с риском.

Передача риска означает, что ответственность за риск передается кому-то другому, например, страховой компании.

Снижение степени риска - это сокращение вероятности и объема потерь.

Для этого применяют различные приемы:

-диверсификация;

-хеджирование;

-самострахование;

-прогназирование.

Оценка риска и его минимизация

В основе анализа риска лежит определение того, **что надо защищать, от кого и как**. Для этого выявляются **активы АС**, нуждающиеся в защите

Категории активов	Компоненты АС
Аппаратное обеспечение	Компьютеры, периферийные устройства, коммуникационные линии, сетевое оборудование и их составные части
Программное обеспечение	Исходные, объектные и загрузочные модули операционных систем, вспомогательных системных и коммуникационных программ, инструментальных средств разработки, прикладных программных пакетов
Информационное обеспечение	Вводимые и обрабатываемые, хранимые, передаваемые и резервные (сохранные копии) данные и метаданные
Персонал	Обслуживающий персонал и пользователи
Документация	Конструкторская, техническая, пользовательская и иная документация
Расходные материалы	Бумага, магнитные носители, картриджи и т.д.

Источники угроз активам АС

Внешние источники угроз	Внутренние источники угроз
1.Атмосферные явления, стихийные бедствия, катастрофы, аварии, 2.Деятельность конкурирующих экономических структур, 3.Деятельность преступных группировок и лиц и др.	1.Нарушение персоналом режимов безопасности 2.Отказы и сбои аппаратных средств и носителей информации, 3.Ошибки программного обеспечения, 4.Деятельность преступных группировок и лиц и др.

На этапе анализа вариантов проекта оценивается их рискованность

Степень риска - это вероятность наступления случая потерь, а также размер возможного ущерба от него.

Определяются основные виды и степень риска.

- **Строится кривая риска.**
- **Планируется меры по снижению риска.**

Технико-экономические задачи защиты информации на предприятии

1.Анализ

Оценка возможного ущерба (потерь) при нарушении или недостаточной защищенности информации.

Определение допустимых расходов на защиту информации (ЗИ).

Определение технико-экономических показателей проекта системы ЗИ.

2.Синтез

Проектирование систем ЗИ, удовлетворяющих одному из двух условий:

-**обеспечение максимально возможного уровня защиты информации при заданном расходовании ресурсов;**

-**достижение заданного уровня ЗИ при минимальном расходовании ресурсов.**

3.Управление

Обоснование планов функционирования систем ЗИ, оптимальных по технико-экономическим показателям (ТЕП).

Оптимизация по ТЕП оперативно-диспетчерского управления защитой информации.

Оптимизация по ТЕП календарно-планового руководства функционированием системы ЗИ.

Оптимизация ТЕП организационно-структурного построения органов ЗИ.

Оптимизация по ТЕП арсенала средств ЗИ.

Создание оптимальной СЗИ

Построение оптимальной системы защиты может быть реализовано следующим подходом:

1. **На основе опыта создания систем защиты информации, составляются варианты наборов задач защиты.**
2. **Определяются наиболее подходящие наборы средств, использованием которых могут быть решены различные задачи защиты на различных рубежах.**
3. **На основе технико-экономических оценок средств защиты определяются размеры ресурсов, необходимых для практического использования различных средств.**

Анализ защищенности объекта

Для определения слабых мест в защите используют метод моделирования угрожающей ситуации:

1. **Незнакомый для охраны человек ходит вокруг здания, фотографирует объект, делает пометки в блокноте. При этом скрытно оценивается реакция охраны.**
2. **Человек под видом курьера приносит и передает охране посылку с просьбой передать руководителю.**
3. **Делается попытка проникнуть на объект под видом электрика, сантехника и т.д.**
4. **К разным должностям вносится кейс и оставляется (проверяется реакция СБ).**
5. **В местах сосредоточения коммуникаций прикрепляется к стене коробочка (ведется наблюдение за поведением обслуживающего персонала).**
6. **Котролируемый подкуп персонала.**

Экономическая безопасность предприятия

Эффективное использование ресурсов предприятия возможнолишь в условиях общей **экономической безопасности**, где **информационная безопасность** является одной из составляющих.

Экономическая безопасность предприятия это состояние эффективного использования ресурсов предприятия для предотвращения угроз и обеспечения его стабильного функционирования и развития.

Составляющие экономической безопасности предприятия

Экономическая безопасность предприятия имеет 7 составляющих:

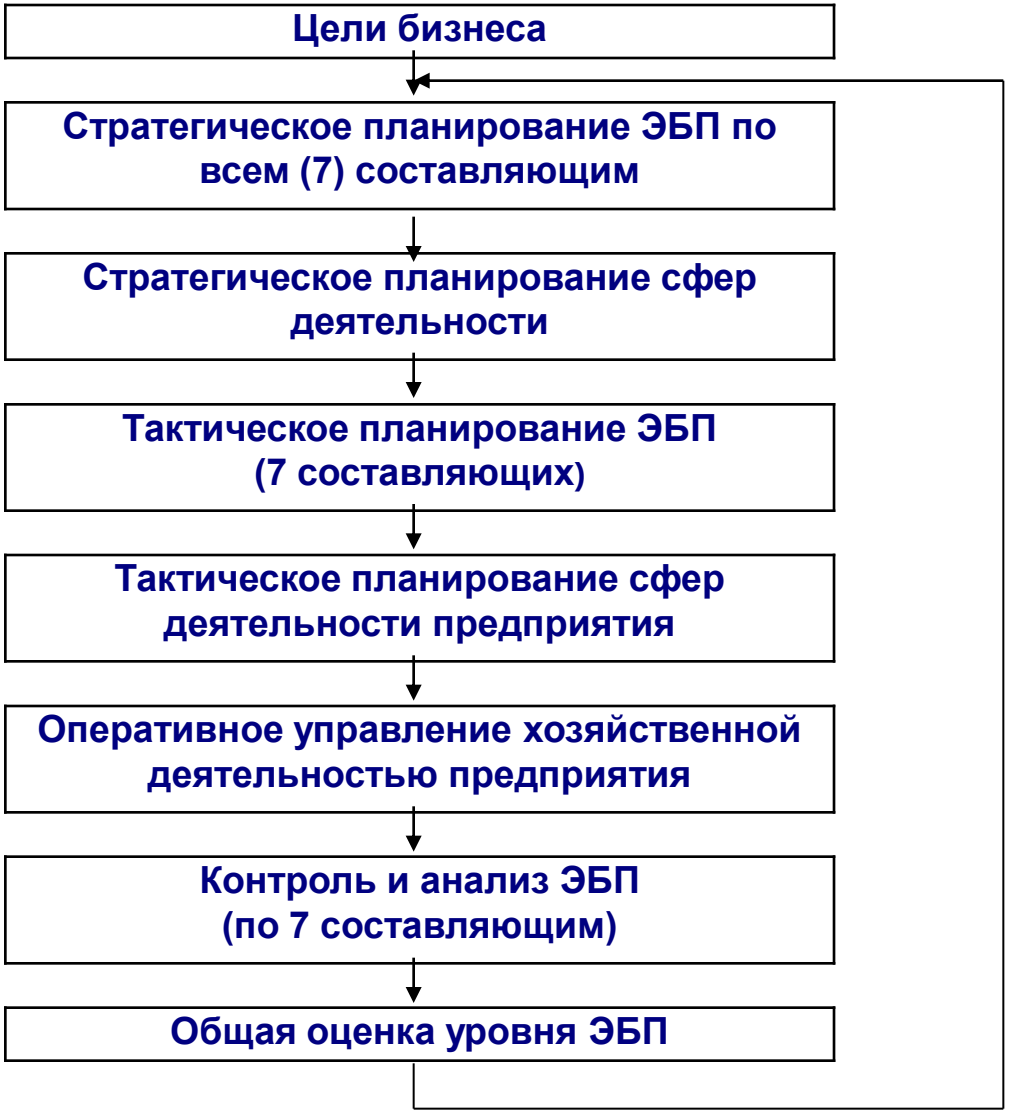
- финансовая,
- кадровая,
- правовая,
- технологическая,
- экологическая,
- информационная,
- силовая.

Для обеспечения своей экономической безопасности предприятие использует следующие ресурсы:

капитала,
прав,
информационный.
персонала,
техники,

При условии эффективного использования природных ресурсов

Схема процесса обеспечения ЭБП



Оценка экономической безопасности предприятия

Оценка уровня экономической безопасности предприятия определяется с помощью расчета **совокупного критерия экономической безопасности (Ск)** по формуле:

$$Ск=\sum_{1}^{N} Кidi\ ,$$ где

$Ki= U1i /(Si+U2i) \longrightarrow$ max, значение критерия i-й составляющей экономической безопасности предприятия;

U1i-предотвращенный ущерб по i-й составляющей;

U2i-понесенный ущерб по i-й составляющей;

Si-затраты на реализацию мер по предотвращению ущерба по i-й составляющей;

di-удельные веса значимости критериев, причем d1+d2+...+dn=1.

Пример расчета значения критериев для промышленных предприятий

Составляющие экономической безопасности	Финан-совая	Интеллек-туальная	Техноло-гическая	Право-вая	Информа-ционная	Экологи-ческая	Силовая
Удедьный вес значимости (di)	0,2	0,1	0,3	0.1	0,15	0.1	0,05
К (предпр. А)	1,83	2,17	0,74	0,82	1,6	0,92	1
К (предпр. В)	1,14	0,81	1,32	0,63	0,97	1,72	0,54
К (предпр. С)	0,82	2,43	1,56	1,22	1,87	2,69	1,93
СК (пр. А)	1,372						
СК (пр. В)	1,06						
СК (пр. С)	1,73						

/Основы экономической безопасности. Под ред. Олейникова Е.А. М.: ЗАО "Бизнес-школа Интел-Сервис", 1997/

Критерии создании системы ЭБП объекта

1. Политику ЭБП должны определять собственники капитала, а не сотрудники служб безопасности.
2. Обеспечение ЭБП должно быть в рамках целевой программы, иметь системный характер.
3. Любые нарушения в деятельности фирмы должны рассматриваться как угроза ЭБП.
4. Система ЭБП должна быть индивидуальной.
5. ЭБП должна базироваться на принципе законности.
6. ЭБП должна быть экономически обоснована (затраты на систему защиты должны составлять не менее 20-25% от прибыли).
7. Обеспечение необходимого уровня безопасности всех 7-и составляющих ЭБП.