МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по выполнению практических работ
по дисциплине «УПРАВЛЕНИЕ ПРОЕКТАМИ ПО ЗАЩИТЕ ИНФОРМАЦИИ И ЭКОНОМИКА ЗАЩИТЫ ИНФОРМАЦИИ»
для студентов специальности 10.05.01 Компьютерная безопасность
специализация «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Ставрополь
2026

СОДЕРЖАНИЕ

Практическая работа №1. Система управления проектами. Предварительная проработка целей и задач проекта……3
Практическая работа №2. Окружение проектов. Классификация понятий и типов проектов. Цели, стратегия, результаты и параметры проектов…….8
Практическая работа №3 Планирование потребности и использование ресурсов по стадиям проекта и требованиям заказчика…….11
Практическая работа №4. Детальное планирование. Документирование плана проекта Угрозы невыполнения проектов…….16
Практическая работа №5 Создание и оформление графика работ и просмотр критического пути диаграмма Ганта……..21
Практическая работа №6 Способы обеспечения целостности данных по проекту. Ввод таблицы ресурсов и участников проекта……31
Практическая работа №7. Решение проблемы перегрузки ресурсов по проекту информационной безопасности. Способы оптимизации графика работ……40
Практическая работа № 8. Отслеживание хода выполнения работ и фактических затрат по проекту в любой профессиональной сфере. Защита уровней обеспечения выполнения графика проекта……..58
Практическая работа №9 Различные виды просмотра информации в проекте любой сферы, вывод отчётных данных проекта Специалисты в области управления проектами. Расчет капитальных вложений……..62

Практическая работа №1. Система управления проектами.
Предварительная проработка целей и задач проекта

Цель работы

- Закрепить теоретические знания
- Изучить метод планирования бюджета на защиту информации

Подготовка к работе

При домашней подготовке лабораторной работы необходимо подготовить отчет, содержащий:

- титульный лист с указанием варианта задания;
- цель работы;
- таблицы №1 и №2;
- для выполнения работы, необходимо изучить теоретический материал по изучению планирования бюджета на защиту информации.

Ход занятия

1. Проверка готовности студентов к работе.
2. Проверка знаний теоретического материала и порядка выполненияработы.
3. Выполнение лабораторной работы.
4. Составление отчета.

Теоретическая часть.

При разработке плана защиты информации после учета всех ее носите лей и возможных источников, потери целесообразно проанализировать соотношением планируемых затрат с возможными потерями, если все же утечка или утрата информации произойдет. Наибольшую трудность представляет подсчет возможных потерь от информационного ущерба. В ряде случаев выгода конкурента может быть выше, чем ваши собственные потери. Для учета указанных обстоятельств разработана методика. Ее суть и том, что затраты, выделяемые на противодействие каждой угрозе, распределяются в зависимости от интегрального показателя: прогнозируемого при ее реализации соотношения выгоды конкурента и собственных потерь. В результате ранжирование угроз осуществляется не по их прогнозируемой вероятности осуществления,а с учетом данного интегрального показателя. Для этого учета выполняется ряд операций.

Руководством организации выявляется i-ое количество угроз с различной вероятностью осуществления на планируемый период. С привлечением экспертов оценивается вероятность осуществления каждой угрозы **Pi.** Следует подчеркнуть, что вероятность угрозы – величина, неадекватная величине потери от неё и не пропорциональная ей. Угрозы на нижнем и среднем уровне организационной системы предприятия (**I1, I2…**), как правило, имеют большие значения вероятностей ведь на этих уровнях больше сотрудников, контактов, технических средств и т.п. Все это трудно контролировать, весьма проблематично разграничивать доступ к информации. Однако угрозы, реализованные на нижнем уровне (**Ii**), как правило, приводят не к самым большим собственным потерям и таким же выгодам конкурентов. Угрозы на верхнем уровне организационной структуры имеют меньшую вероятность, но собственные потери могут быть значительными (**D_{co6}**), а выгоды конкурента и того выше (**D_{co6}**), так как здесь сосредоточены основные массивы инновационной информации.

Затем учитывается влияние соотношения потерь и выгод на вероятностную характеристику угрозы по каждой угрозе. Для этого значение вероятности угрозы возводится в степень, равную отношению собственных потерь к величине выгоды конкурента при реализации, данной угрозы.

Величину угрозы вероятности будем называть *весом угрозы*, сущность которого заключается в следующем: рост потенциальной выгоды конкурента приводит к росту затрат на защиту от данной угрозы в сумме общих затрат. $P_{весі} \bullet P^{\vee} i$

Затем учитывается соотношение потерь и выгод от всей совокупности угроз. Для этого вес каждой угрозы умножается на относительную величину отношение суммы собственных потерь и выгод конкурента от данной угрозы к общей сумме собственных потерь и выгод конкурентов от всех угроз.

$$P_{отні} \bullet (D_{собі}\ D_{коні}) / (\Sigma D_{собі} \cdot \Sigma D_{коні})$$

Произведение веса угрозы на это отношение потерь и выгод будем называть *значимостью защиты* от данной угрозы, значение которой и будет показывать долю отчисления от общей суммы, выделяемую на противодействие каждой угрозе.

$$P_{зні} \bullet P_{весі} * P_{отні}$$

После расчета значимости от каждой угрозы проводится итоговое ранжирование по следующим параметрам:

- По уровням организационной структуры
- По значению вероятности угрозы
- По значению веса угрозы
- По значению значимости защиты

Затем необходимо подсчитать величину средств, необходимую на защиту информации от прогнозируемых угроз.

$$D_{н.от} \bullet 0.3 * \Sigma D_{собі}$$

Данная доля от сберегаемой прибыли предназначена для нейтрализации суммы значимостей всех угроз:

$$D_{н.отi} \ P_{зн.i}$$

Распределение сумм находится применением следующего выражения:

$$D_{н.отi} \bullet D_{н.от} * P_{зні} / \Sigma P_{зні}$$

Индивидуальные задания

Руководством предприятия выявлено пять угроз **I**1…**I**5 с различной вероятностью осуществления на планируемый период. С привлечением экспертов оценили вероятность осуществления каждой угрозы P1…P5, собственные потери (в виде не полученной прибыли) Dсоб. , а так же полученные при этом выгоды конкурентов Dкон.

Требуется найти: величину суммы, которая должна быть выделена на защиту информации, и ее распределение на мероприятия по защите от каждой угрозы с учетом возможных собственных потерь и приобретений конкурентов. Результаты расчетов поместить в таблицу (1).

Произвести ранжирование угроз по следующим параметрам:

- По уровням организационной структуры
- По значению вероятности угрозы
- По значению веса угрозы
- По значению значимости защиты. (результаты поместить в таблицу №2)

Приложение

Таблица 1

№ П/п	Параметры	Угроза Ii					Суммы
		I1	**I**2	**I**3	…	**I**i	
1	Значение вероятности угроз Pi						———
2	Собственные потери (прибы ли) Dособі, в тыс.						
3	Выгоды (прибыли) конкурентов Dконі, в тыс.						
4	Показатель степени $_i$ в формуле веса						———
5	Вес угрозы Рвесі						———
6	Суммы собственных потерь и выгод конкурентов.						
7	Относительный вес потерь Ротні						
8	Значимость защиты от угрозы Рзні						
9	Значения сумм на противодействие каждой угрозе **D**н.от.і.						

Таблица 2. Ранжирование угроз

По уровням организационной структуры					
По значению вероятности угрозы					
По значению веса угрозы					
По значению значимости угрозы					

Варианты заданий

Вариант №1

Параметры	Угроза Ii				
	I1	**I**2	**I**3	**I**4	**I**5
Значение вероятности угроз Pi	0,7	0,8	0,9	0,6	0,5
Собственные потери (прибыли) Dособі, в тыс.	100	200	100	300	100
Выгоды (при были) конкурентов Dконі, в тыс.	100	400	200	200	400

Вариант №2

Параметры	Угроза Ii				
	I1	**I**2	**I**3	**I**4	**I**5
Значение вероятности угроз Pi	0,8	0,7	0,9	0,6	0,5
Собственные потери (прибыли) Dособі, в тыс.	200	100	500	200	300

Выгоды (при были) конкурентов Dконі, в тыс.	100	400	100	200	600

Вариант №3

Параметры	Угроза Ii				
	I1	**I**2	**I**3	**I**4	**I**5
Значение вероятности угроз Pi	0,9	0,7	0,8	0,5	0,6
Собственные потери (прибыли) Dособі, в тыс.	300	500	100	400	100
Выгоды (при были) конкурентов Dконі, в тыс.	600	300	300	700	200

Вариант №4

Параметры	Угроза Ii				
	I1	**I**2	**I**3	**I**4	**I**5
Значение вероятности угроз Pi	0,9	0,7	0,8	0,5	0,6
Собственные потери (прибыли) Dособі, в тыс.	300	500	100	400	100
Выгоды (при были) конкурентов Dконі, в тыс.	600	300	300	700	200

Вариант №5

Параметры	Угроза **I**i				
	I1	**I**2	**I**3	**I**4	**I**5
Значение вероятности угроз Pi	0,9	0,7	0,8	0,5	0,6
Собственные потери (прибыли) Dособі, в тыс.	300	400	150	200	300
Выгоды (при были) конкурентов Dконі, в тыс.	500	300	300	400	400

Вариант №6

Параметры	Угроза **I**i				
	I1	**I**2	**I**3	**I**4	**I**5
Значение вероятности угроз Pi	0,8	0,9	0,7	0,5	0,6
Собственные потери (прибыли) Dособі, в тыс.	100	200	200	300	150
Выгоды (при были) конкурентов Dконі, в тыс.	100	400	500	400	200

Вариант №7

Параметры	Угроза **I**i				
	I1	**I**2	**I**3	**I**4	**I**5
Значение вероятности угроз Pi	0,7	0,9	0,8	0,6	0,5
Собственные потери (прибыли) Dособі, в тыс.	300	400	200	100	500
Выгоды (при были) конкурентов Dконі, в тыс.	600	100	900	500	200

Контрольные вопросы:

1. Почему угрозы на нижнем и среднем уровне организационной системыпредприятия имеют большие значения вероятностей?
2. Что показывает интегральный показатель?
3. Что характеризует вес угрозы?
4. Что называется значимостью защиты от данной угрозы?

Практическая работа №2. Окружение проектов. Классификация понятий и типов проектов. Цели, стратегия, результаты и параметры проектов.

Цель работы

- Закрепить теоретические знания
- Изучить метод количественной оценки риска.

Подготовка к работе

При домашней подготовке лабораторной работы необходимо подготовить отчет, содержащий:

- титульный лист с указанием варианта задания;
- цель работы;
- для выполнения работы, необходимо также изучить теоретический материал по количественной оценки риска с помощью методов математической статистики, а так же познакомиться с приемами снижения степени риска.

Ход занятия

1. Проверка готовности студентов к работе.
2. Проверка знаний теоретического материала и порядка выполненияработы.
3. Выполнение лабораторной работы.
4. Составление отчета.

Теоретическая часть.

Под риском принято понимать вероятность (угрозу) потери предприятием части своих ресурсов, недополучения доходов или появления дополнительных расходов в результате осуществления определенной производственной и финансовой деятельности.

Эффективность организации управления риском во многом определяется знанием его разновидностей. С экономической точки зрения интересны не все виды рисков, а лишь те, которые влияют на экономическое положение предприятий.

Чистые риски это природно-естественные, экологические, политические, транспортные и часть коммерческих рисков (имущественные, производственные, торговые).

Особое значение приобретает анализ и оценка предпринимательского риска. Цель анализа риска заключается в том, чтобы представить необходимую информацию руководству для принятия решений о целесообразности инвестиций и предусмотреть меры по защите от возможных потерь.

Существуют следующие методы анализа риска:

-статистический;

-анализ целесообразности затрат;

-аналитический;

-экспертных оценок;

-аналогий.

Чтобы количественно определить величину риска, необходимо знать возможные последствия какого-нибудь отдельного действия и вероятность самих последствий.

Таким образом, математическое ожидание какого-либо события равно абсолютной величине этого события, умноженной на вероятность его наступления.

Избежание риска означает уклонение от мероприятий, связанных с риском. Снижение степени риска это сокращение вероятности и объема потерь. Для этого применяют различные приемы. Наиболее распространенными являются:

диверсификация;

хеджирование;

самострахование;

страхование.

Диверсификация производственной деятельности заключается в распределении усилий и капиталовложений между разнообразными видами деятельности, непосредственно не связанными друг с другом. В таком случае если в результате непредвиденных событий один вид деятельности будет убыточным, другой вид все же будет приносить прибыль. Следует различать концентрическую и горизонтальную диверсификацию. Концентрическая диверсификация это пополнение ассортимента изделиями, похожими на продукцию уже выпускаемую предприятием. Горизонтальная диверсификация представляет собой пополнение ассортимента изделиями, не похожими на товары предприятия, но интересными для потребителей. Метод диверсификации позволяет снижать производственные, коммерческие и инвестиционные риски.

В последнее время с развитием рыночных отношений появились новые формы торговых сделок. В связи с этим у предприятий появился новый способ компенсации возможных потерь от риска — *хеджирование* (от английского hedging — ограждать). Хеджирование, как правило, используется для минимизации рисков снабжения в условиях высоких инфляционных ожиданий и отсутствие надежных каналов закупок. В самом общем виде хеджирование можно определить, как страхование цены товара от риска, либо нежелательного для производителя падения, либо невыгодного потребителю увеличения путем создания встречных валютных, коммерческих, кредитных и иных требований и обязательств. Таким образом, хеджирование может использоваться предприятием с целью страхования прогнозируемого уровня доходов путем передачи риска другой стороне.

Приемлемым для предприятия вариантом минимизации риска может стать *самострахование* некоторых видов рисков, т.е. есть создание специального резервного фонда (фонда риска) за счет отчисления от прибыли, на случай возникновения непредвиденной ситуации. Самострахование целесообразно в том случае, когда стоимость страхуемого имущества относительно невелика по сравнению с общим объем капитала предприятия. Например, крупному предприятию не выгодно через страховую компанию страховатьне дорогое оборудование. Самострахование имеет также смысл, когда вероятность убытка достаточно мала.

Страхование представляет собой одну из экономических категорий производственных отношений. *Его сущность заключается в распределении ущерба между всеми участниками страхования.* Оно связано с возмещением материальных потерь, что служит основой для непрерывности и бесперебойности процесса воспроизводства.

Особый интерес представляет количественная оценка риска с помощью методов математической статистики. Главные инструменты данного метода оценкиматематическое ожидание дискретной случайной величины, среднее квадратическое отклонение, дисперсия дискретной случайной величины, коэффициент вариации.

Дискретной (прерывной) называют случайную величину, которая принимает отдельные, изолированные возможные значения с определенными вероятностями.

Математическим ожиданием дискретной случайной величины называют сумму произведений всех ее возможных значений на их вероятности.

Дисперсией дискретной случайной величины называют математическое ожидание квадрата отклонения случайной величины от ее математического ожидания.

Средним квадратическим отклонением случайной величины называют квадратный корень из дисперсии.

Задание:

В результате аудита корпорации и 20 ее филиалов было выявлено, что в каждом филиале ежемесячно происходит утечка информации. Необходимо рассчитать количественную оценку риска общей потери информации в каждом филиале. Сравнить полученную оценку с порогом потери информации в 40%, начертить график.

Данные по проверке представлены в таблице №1 за пять месяцев.

Месяц Филиал	январь	февраль	март	апрель	май
№1	43	10	50	15	25
№2	50	15	12	32	45
№3	28	10	20	31	12
№4	10	30	25	45	18
№5	13	45	24	30	10
№6	5	25	10	40	38
№7	50	15	12	25	18
№8	26	36	8	14	25
№9	35	15	22	45	14
№10	23	20	18	27	30
№11	25	9	23	10	50
№12	16	10	12	36	25
№13	38	32	25	22	15
№14	10	20	6	46	30
№15	37	18	30	8	14
№16	10	16	28	20	26
№17	45	10	16	34	36
№18	15	23	14	26	12
№19	28	45	23	14	10
№20	31	15	21	30	15

Контрольные вопросы:

1. Какая величина называется дискретной случайной величиной?
2. Что такое математическое ожидание?
3. Что характеризует дисперсия?
4. Какие приемы применяют для снижения степени риска?
5. В чем заключается метод хеджирования?
6. Что такое диверсификация?

Практическая работа №3 Планирование потребности и использование ресурсов по стадиям проекта и требованиям заказчика.

Цель работы

- Закрепить теоретические знания.
- Изучить модель определения зон защиты в условиях ограниченности защитных средств.
- Изучить модель распределения поисковых усилий подразделенияслужбы безопасности предприятия.

Подготовка к работе

При домашней подготовке лабораторной работы необходимо подготовить отчет, содержащий:

- титульный лист с указанием варианта задания;
- цель работы;
- начертить сетку таблицы №1;

для выполнения работы, необходимо изучить теоретический материал по игровым моделям определения зон и средств защиты предприятия от угроз; повторить методы линейного программирования (например, симплекс-метод), графический метод.

Ход занятия

1. Проверка готовности студентов к работе.
2. Проверка знаний теоретического материала и порядка выполнения работы.
3. Выполнение лабораторной работы.
4. Составление отчета.

Теоретическая часть.

Особое внимание необходимо уделять исследованию возможностей предприятия по профилактике, предотвращению и локализации угроз его экономической безопасности в виде хищений и повреждений документации, информационных технологий и программных продуктов. Защита от угроз и угрозы есть явления, в которых участвуют две противоположные стороны со своими экономическими интересами, целями и путями их достижения. Такие явления принято называть конфликтами. Ход событий в конфликте между предприятием, с одной стороны и угрожающими структурамис другой, зависит от решений, принимаемых каждой из сторон. Для конфликта характерно то, что никто заранее не знает, какие решения примут другие участники, т.е. все вынуждены действовать в условиях неопределенности. Формализация содержательного описания конфликта представляет собой его математическую модель, которую называют игрой. Участники рассматриваемого конфликта игроки. Конфликт между сторонами антагонистический, он может моделироваться антагонистической игрой, исход которой оценивается вещественным числом. Значение исхода одна из сторон стремиться максимизировать (игрок 1), а другая минимизировать (игрок 2). Отсюда выигрыш одной из сторон составляет проигрыш противоположной стороны.

Общая игровая модель определения зон защиты формулируется следующим образом. Предположим, что может возникнуть один из n нежелательных для предприятия видов угроз его безопасности. В свою очередь, предприятие может применить один из n способов защиты от этих угроз. Если под полезностью структуры, пытающейся снять информацию, понимать ущерб, который она причиняет предприятию, то конфликт можно моделировать антагонистической игрой. Эта игра определяется матрицей выигрышей H :
Здесь x1,x2,..xn, y1; y2…yn-соответственно частоты вероятности, в которых смешиваются чистая стратегия игроков 1 и 2; ~ цена игры. При небольшой размерности игры ее можно

реализовать из непосредственного решения систем уравнений (1) и (2). Если же игра сложная, то для ее реализации можно использовать методы линейного программирования (например, симплексметод).

Применительно к конкретным условиям взаимосвязи предприятия с возможными угрозами можно представить различные игровые модели определения зон и средств их защиты. Очень интересной и наиболее часто встреча ющейся является *модель «Определения зон защиты в условиях ограниченности защитных средств».* Пусть одно из предприятий, на котором есть n защитных зон (объектов) и на которое воздействуют внешние угрозы, располагает ограниченным количеством средств, которые можно использовать для защиты только одной зоны. Ценность (полезность) зоны может быть выражена в стоимости информации, в случае ее потери и составляет bi (I=1..n).

Тогда математическое ожидание ущерба, наносимого предприятию, при выборе различными сторонами зон I и j можно рассчитать по формуле:

$$z_{ij} = \begin{cases} b_i * (1 - p), если (i \neq j; i, j = 1, n) \\ b_i, если i = j; (i, j = 1, n) \end{cases}$$

где p вероятность неуничтожения зоны, p<1.

Рассматриваемый конфликт моделируется конечной антагонистической игрой, матрица выигрышей которой имеет вид:

$$H = \begin{pmatrix} (1-p)*b_1 & b_1 & \ldots & b_1 & \ldots & b_1 \\ b_2 & (1-p)*b_2 & \ldots & b_2 & \ldots & b_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ b_n & b_n & \ldots & (1-p)*b_n & \ldots & b_n \end{pmatrix}$$

Для игрока 2 (предприятие) эта игра описывается системой неравенств:

$$\begin{cases} (1-p)*b_1*y_1 + b_1*y_2 + \ldots + b_1*y_n \geq 1 \\ b_2*y_1 + (1-p)*b_2*y_2 + \ldots + b_2*y_n \geq 1 \\ \ldots \\ b_n*y_1 + b_n*y_2 + \ldots + (1-p)*b_n*y_n \geq 1 \\ y_1 + y_2 + \ldots + y_n = 1 \end{cases},$$

далее

$$\begin{cases} (1-p)*b_1*t_1 + b_1*t_2 + \ldots + b_1*t_n \geq 1 \\ b_2*t_1 + (1-p)*t_2 + \ldots + b_2*t_n \geq 1 \\ \ldots \\ b_n*t_1 + b_n*t_2 + \ldots + (1-p)*b_n*t_n \geq 1 \\ t_1 + t_2 + \ldots + t_n \to \max \\ t_1, t_2 \ldots, t_n \geq 0 \end{cases},$$

где $y = \frac{1}{t_1 + t_2 + \ldots + t_n}$,

$i \quad i \quad = \quad .$

Эту задачу можно решить симплекс-методом, графическим методом или любым другим способом.

Рассмотрим *модель распределения поисковых усилий подразделения службы безопасности предприятия.* Задача службы безопасности предприятия состоит в том, чтобы не только организовать защиту его зон, но и отыскивать возможные варианты нападений. Пусть на предприятии есть n зон возможного нападения. Предполагается, что в одной из зон организована криминальная группа. Для ее выявления в оргструктуре предприятия предусмотрено специальное подразделение из L человек. Если в группу входит по $\ddagger$ человек, то число таких подгрупп равно $r \bullet L / \ddagger$. Эти подгруппы службы безопасности можно распределить по зонам по-разному. Все r подгрупп могут действовать в первой зоне или в первую зону можно послать (r-1) подгруппу, во вторую зону одну подгруппу, в остальные ни одной, или другим произвольным образом. Очевидно, что вероятность того, что одна подгруппаобнаружит криминальную структуру в j-й зоне, зависит от многих условий, характеризующих эту зону. Обозначим такую вероятность через wj и будем считать, что обнаружение каждой подгруппой службы безопасности действия криминальной структурынезависимые события. Обычно противоборствующие стороны располагают априорной информацией о значениях wj (j=1..n), и поэтому каждая из них может определить вероятность обнаружения криминальной структуры в j-ой зоне по формуле:

$$h_{i,j} \bullet \tilde{1} \ (\tilde{1} \ w \ )^{q_j}$$

где q_j число подгрупп службы безопасности, действующих в j-ой зоне.

Предприятие (игрок 1) должно распределить подгруппы службы безопасности по зонам, криминальная структура (игрок 2)выбрать зону своих действий. Следовательно имеется конфликт двух сторон. Игрок 1 распределяет подгруппы службы безопасности, рассчитывая максимизировать вероятность обнаружения действий криминальной структуры. Игрок 2 выбирает зону нападения, рассчитывая минимизировать эту вероятность. Очевидно, что игроки преследуют противоположные цели и поэтому конфликт антагонистичен, т.е. выигрыш игрока 1 равен проигрышу игрока 2. Данную игру можно задать матрицей:

$$H \bullet \begin{pmatrix} h_{11} & \ldots & h_{1n} \\ h_{21} & \ldots & h_{2n} \\ \ldots & \ldots & \ldots \\ h_{m1} & & h_{mn} \end{pmatrix}$$

где mчисло чистых стратегий игрока1; nчисло чистых стратегий игрока 2;
hij=H(I,j)-выигрыш игрока 1 в ситуации (I,j).

Чистой стратегией игрока 1 является вектор $i \bullet (q^i, q^i, \ldots, q^i)$, компонен1 2 n ты которого q^i_j $0, r$ целые неотрицательные числа, число подгрупп служ-бы безопасности, направляемых в j-ю зону согласно I-ой чистой стратегии:

$$n \quad q^i \bullet r, \qquad 1 \boxtimes i \boxtimes m$$

$$j$$

$$j \bullet 1$$

Число чистых стратегий игрока 1 равно числу сочетаний с повторением из (n+r-1) элементов по r элементов, т.е.

$$m \bullet \overset{r}{\underset{n\tilde{r}1}{}} \bullet \frac{(n\ \tilde{r}\ 1)!}{r!*(\tilde{n}\ 1)!}$$

Чистой стратегией игрока 2 является выбор зоны нападения. Полезностью нападающей стороны (игрока 1), очевидно, будет вероятность обнаружениякриминальной структуры в j-ой зоне, которая определяется:

$$h_{i,\ j} \bullet \tilde{1}\ (\tilde{1}\ w_j)^{\ q^i_j}$$

Далее составляется таблица:

Стратегия игрока 1	Стратегия игрока 2 (конкурентной структуры)		
	1	…..	n
1			
2			
…			
$C^n_{n\tilde{r}1}$			

После заполнения таблицы составляется матрица выигрышей H. Математические стратегии игроков определяются решением систем уравнений.

Задания.

Задача 1. Максимальная стоимость информационных ресурсов, имеющихся на предприятии, составляет на первом уровне *b1*, на втором *b2* и на третьем *b3*. Предполагается, что вероятность незащищенности информационных ресурсов *p*. Предприятие располагает ограниченным количеством средств, которые можно использовать для защиты только одной зоны. Просчитать веро ятности необходимости защиты каждой из зон.

Вариант №1
b1=320
b2=430
b3=300
p=40%

Вариант №2
b1=150
b2=120
b3=100
p=50%

Вариант№3
b1=170
b2=200
b3=150
p=50%

Вариант №4
b1=230
b2=185
b3=160
p=50%

Вариант №5
b1=230
b2=300
b3=220
p=35%

Задача 2. На предприятии есть три зоны возможного хищения или повреждения документации, функционирует подразделение службы безопасности численностью в 12 человек, которое разделено на 3 равновеликих группы.
Вероятность обнаружения криминальной структуры одной группой задается

экспертными оценками параметров *w1*, *w2*, *w3*. Каким образом необходимо распределить подгруппы службы безопасности по зонам поиска возможногохищения.

Вариант №1	*Вариант №2*	*Вариант№3*
w1=0.5	w1=0.5	w1=0.4
w2=0.4	w2=0.3	w2=0.5
w3=0.7	w3=0.2	w3=0.1

Вариант №4	*Вариант №5*
w1=0.4	w1=0.6
w2=0.3	w2=0.4
w3=0.7	w3=0.1

Контрольные вопросы:

1. Что представляет собой игра?
2. Написать общий вид матрицы выигрышей H?
3. Сформулировать общую постановку задачи для модели распределенияпоисковых усилий подразделения службы безопасности предприятия?
4. Сформулировать общую постановку задачи для модели определениязон защиты в условиях ограниченности защитных средств?
5. Написать формулу вычисления числа сочетаний с повторением?

Практическая работа №4. Детальное планирование. Документирование плана проекта Угрозы невыполнения проектов.

Цель работы

- Закрепить теоретические знания.
- Научиться различать оперативную, тактическую и стратегическую информацию.
- Изучить основные рекомендации при организации проверки и отбора кандидатов на работу в коммерческие предприятия.

Ход занятия

1. Проверка готовности студентов к работе.
2. Проверка знаний теоретического материала и порядка выполнения работы.
3. Выполнение лабораторной работы.
4. Обработка результатов.

Теоретическая часть.Информация фирмы.

Существуют различные подходы классификации информации, накапливаемой и циркулирующей на фирме. С одной стороны, ее можно разделитьна два больших блока:

Технологическую информацию, характеризующую научно техническую сторону производства, «ноу-хау», часть которой представляет предмет пристального внимания конкурентов и промышленных шпионов;

деловую информацию, связанную с управленческой, финансовой, маркетинговой и т.п. деятельностью, позволяющей успешно вести дела и заключать взаимовыгодные сделки.

С другой стороны, информация, необходимая для принятия решений и потребляемая фирмой, может быть разделена на три группы:

- информация для стратегических решений;
- информация для тактических решений:
- информация для оперативных решений.

Для получения надлежащей информации необходимо выбрать базы для наблюдения, которые предопределяются насущными потребностями, те в свою очередь предопределяются поставленными целями. В этом заключается принцип "ЗВ" (buts-besoins-bases) *цели ~ потребности базы.*

Подготовка информации для принятия любого решения должна начинаться с определения целей, которые предопределяют потребности в информации, а затем и базы для наблюдения.

Стратегические цели (строительство новых предприятий, внедрение новой технологии, запуск в производство новой продукции) оказывают кардинальные изменения на функционирование фирмы. Эти цели предопределяют все последующие действия.

Стратегические потребности. Они включают в себя все, что может оказать долгосрочное влияние на деятельность предприятия.

На основании выявленных потребностей следует составить картотеку направлений для наблюдения. Примером могут служить следующие направления:

1. Тенденции по странам.
2. Технологический процесс (сырье, производственные технологии,окружающая среда)
3. Действующие лица
   конкуренты (действительные и потенциальные);
   союзники и партнеры;

кадры.

4. Диверсификация.

Информация для тактических решений

Тактическая цель заключается в выборе наилучшего средства достижения стратегической цели и в контроле неизменности условий, которые предопределили этот выбор.

Тактические потребности. Это может быть и выбор пути для достижения тактических целей. Здесь необходимо различать постоянную окружающую среду и переменную окружающую среду. При этом необходимо выбрать как первое, так и второе. Это различие связано с временной шкалой действий.

Потребности первого типа. Для правильного выбора необходимо знать общие характеристики каждой из сфер.

Потребности второго типа. Необходимо постоянно наблюдать за состоянием окружающей среды для своевременного выявления препятствий, которые могут явиться причиной значительных отклонений от намеченного пути.

В первом случае базы создаются по запросу. Во втором случае ведется всеобъемлющее наблюдение за окружающей средой, т. к. неизвестно откуда будут исходить угрозы.

Прежде всего, речь идет об опасностях рынка и, в частности, об определенных действиях конкурентов. Таким образом, небольшой перечень баз наблюдения, учитываемых на стратегическом уровне, удлиняется на тактическом следующими направлениями:

основные области деятельности и виды продукции (нынешние и будущие);

зоны и территории деятельности;

производственные мощности и способ производства;

патентная и лицензионная активность.

Информация для решения оперативных вопросов

На этом уровне стратегическая цель уже определена, путь ее достижения выбран. Теперь необходимо обеспечить, продвижение вперед в наилучших условиях.

Оперативные потребности. Речь идет о благоприятных возможностях или об угрозах. Во всех случаях требуется свежая, точная, надежная и целенаправленная информация, т.к. речь идет о максимально быстром реагировании.

Оперативные базы. Речь идет о ближайшем окружении фирмы, за которым необходимо следить **с** повышенным вниманием. Сюда, естественно, входят конкуренты и, главным образом, их коммерческая политика: ассортимент продукции, цены, рекламные компании и т.п., а также поставщики, клиенты, система торговли, субподрядчики.

Опыт показывает, что серьезная работа может начинаться со следующими базами:

-конкуренция (вся информация по действующим и потенциальным конкурентам);

рынок (вся рыночная информация, вкусы и запросы потребителей,каналы сбыта и т.п.);

технология (производство и использование продукции);

законодательство (вся информация по законодательству, затрагивающему деятельность фирмы);

ресурсы (информация по материально-техническим ресурсам фирмы,по сырью, навыкам, рабочей силе и финансам);

общие тенденции (политические, экономические, социальные, демографические); прочие факторы.

Система стратегической и перспективной информации (ССПИ) выполняет, главным образом, стратегическую роль, а ее деятельность ориентирована на перспективу.

Система тактической и оперативной информации (СТОЙ) использует контакты сотрудников фирмы с внешним миром, а также возможности меж профессиональных встреч, таких как ярмарки, выставки и конференции (только узко специализированные).

Существуют два способа координации деятельности ССПИ и СТОЙ: один в рамках централизованной организационной структуры, другой в рамках децентрализованной.

Информацию, необходимую для работы, предприятие получает из следующих источников.

Канал "Текст". (Общие публикации + специальные публикации и банкиданных). Канал "Фирма". Это контакты предприятия со всеми партнерами. Канал "Консультант". (Общественные службы + консультанты + адми-
нистрация).

Персонал фирмы и его роль в утечке информации

Анализ угроз информации позволил выделить следующие виды угроз информационным ресурсам по возрастанию степени их опасности:
некомпетентные служащие;
хакеры и крекеры;
неудовлетворенные своим статусом служащие;
нечестные служащие;
инициативный шпионаж;
организованная преступность;
политические диссиденты;
террористические группы.

В связи с этим в целях обеспечения информационной безопасности коммерческих структур необходимо уделять особое внимание подбору и изучению кадров, проверке любой информации, указывающей на их сомнительное поведение и компрометирующие связи.

Психологический профотбор преследует следующие основные цели:

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

выявление предрасположенности кандидата к совершению противоправных действий, дерзких и необдуманных поступков;

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

В настоящее время ведущие коммерческие структуры имеют строго разработанные и утвержденные руководством организационные структуры и функции управления для каждого подразделения. Используются оргсхемы или организационные чертежи, на которых графически изображается каждое рабочее место, прописываются должностные обязанности и определяются информационные потоки для отдельного исполнителя.

Кроме того, для большей конкретизации этих процедур на каждое рабочее место составляются профессиограммы.

Профессиограмма это перечень личностных качеств с оценочной шкалой, которыми в идеале должен обладать потенциальный сотрудник. Обязательными атрибутами подобных документов являются разделы, отражающие профессионально значимые качества (психические характеристики, свойства личности, без которых невозможно выполнение основных функциональных обязанностей), а также противопоказания (личностные качества, которые делают невозможным зачисление кандидата на конкретную должность).

Основные рекомендации при организации проверки и отбора кандидатов на работу в коммерческие предприятия.

С точки зрения обеспечения стратегических интересов коммерческой структуры являются обязательными следующие основные функции по отбору кандидатов на работу:

-определение степени вероятности формирования у кандидата преступных наклонностей в случаях возникновения в его окружении определенных благоприятных обстоятельств (персональное распоряжение кредитнофинансовыми ресурсами,

возможность контроля за движением наличных средств и ценных бумаг, доступ к материально-техническим ценностям, работа с конфиденциальной информацией и пр.);

-выявление имевших место ранее преступных наклонностей, судимостей, связей с криминальной средой (преступное прошлое, наличие конкретных судимостей, случаи афер, махинаций, мошенничества, хищений на предыдущем месте работы кандидата и установление либо обоснованное суждение о его возможной причастности к этим преступным деяниям).

Для добывания подобной информации используются возможности различных подразделений коммерческих структур, в первую очередь службы безопасности, отдела кадров, юридического отдела, подразделений медицинского обеспечения, а также некоторых сторонних организаций, например, детективных агентств, бюро по занятости населения, диспансеров и пр. Для сбора сведений такого характера применяются следующие методы: опрос, анкетирование, целевые беседы с лицами по месту жительства кандидатов и на предыдущих местах их учебы или работы, наведение справок через медицинские учреждения, почерковедческая экспертиза и пр.

Используются тщательно подготовленные процедуры приема и увольнения персонала.

Часто имеют место случаи, когда сотрудник внутренне сам уверен в том, что увольняется по откровенно называемой им причине, хотя его решение сформировано и принято под влиянием совершенно иных, поройскрытых от него обстоятельств.

В этой связи принципиальная задача состоит в том, чтобы определить истинную причину увольнения сотрудника, попытаться правильно ее оценить и решить, целесообразно ли в данной ситуации предпринимать попытки к искусственному удержанию данного лица в коллективе либо отработать и реализовать процедуру его спокойного и бесконфликтного увольнения. Поэтому при поступлении устного или письменного заявления об увольнении рекомендуется провести с сотрудником беседу с участием представителей кадрового подразделения и кого-либо из руководителей коммерческой структуры. Однако до беседы целесообразно предпринять меры по сбору следующей информации об увольняемом сотруднике:

-характер его взаимоотношений с коллегами в коллективе;

-отношение к работе;

-уровень профессиональной подготовки;

-наличие конфликтов личного или служебного характера;

-ранее имевшие место высказывания или пожелания перейти на другое место работы;

-доступ к информации, в том числе составляющей коммерческуютайну;

- вероятный период устаревания сведений, составляющих коммерческую тайну для данного предприятия;

- предполагаемое в будущем место работы увольняющегося (увольняемого) сотрудника.

Беседа при увольнении проводиться лишь только после того, когда собраны все необходимые сведения.

В зависимости от предполагаемого результата беседа может проводиться в официальном тоне либо иметь форму доверительной беседы, задушевного разговора» обмене мнениями. Однако каковы бы ни были планы в отношении данного сотрудника, разговор с ним должен быть построен таким образом, чтобы последний ни в коей мере не испытывал чувства униженности, обидны, оскорбленного достоинства. Для этого следует сохранять тон беседы предельно корректным, тактичным и доброжелательным даже несмотря на любые критические и несправедливые замечания, которые могут быть высказаны сотрудником в адрес коммерческой структуры и ее конкретных руководителей.

Если руководством фирмы, отделом кадров и службой безопасности все же принято

решение не препятствовать увольнению сотрудника, а по своему служебному положению он располагал доступом к конфиденциальной информации, то в этом случае отрабатывается несколько вариантов сохранения в тайне коммерчески сведений (оформление официальной подписи о неразглашении данных, составляющих коммерческую тайну, либо устная
«джентльменская» договоренность о сохранении увольняемым сотрудником лояльности к «своему банку или фирме»).

В этой связи необходимо подчеркнуть, что личное обращение к чувству чести и достоинства увольняемых лиц наиболее эффективно в отношении тех индивидуумов, которые обладают темпераментом сангвиника и флегматика, высоко оценивающих, как правило, доверие и доброжелательность.

Что касается лиц с темпераментом холерика, то с этой категорией сотрудников рекомендуется завершить беседу на официальной ноте и тщательно оговаривать и обуславливать в документах возможности наступления для них юридических последствий раскрытия коммерческой тайны.

Несколько иначе рекомендуется действовать в тех случаях, когда увольнения сотрудников происходят по инициативе самих коммерческих структур. Если увольняемое лицо располагает какими-либо сведениями, составляющими коммерческую тайну, то целесообразно предварительно и под соответствующим предлогом перевести его на другой участок работы, например в такое подразделение, в котором отсутствует подобная информация.

Только лишь после реализации этих мер рекомендуется приглашать на собеседование подлежащего увольнению сотрудника и объявлять конкретные причины, по которым коммерческая организация отказывается от его услуг.

После объявления об увольнении рекомендуется внимательно выслушать контр доводы, аргументы и замечания сотрудника в отношении характера работы, стиля руководства компанией и т.д. Обычно увольняемый персонал весьма критично, остро и правдиво освещает ситуации в коммерческих структурах, вскрывая уязвимые места, серьезные недоработки, кадровые просчеты, финансовые неурядицы и т.п.

При окончательном расчете обычно рекомендуется независимо от личных характеристик увольняемых сотрудников брать у них подписку о неразглашении конфиденциальных сведений, ставших известными в процессе работы.

В любом случае после увольнения сотрудников, осведомленных о сведениях, составляющих коммерческую тайну, целесообразно через возможности службы безопасности банка или фирмы (частного детективного агентства) проводить оперативную установку по их новому месту работы и моделировать возможности утечки конфиденциальных данных.

Индивидуальное задание:

1. Определите название вашей фирмы, вид ее деятельности.

2. Составьте перечень информации, являющейся для вашей фирмы оперативной, тактической и стратегической?

3. Составить профили требований (профессиограммы) к любым 2 сотрудникам вашей фирмы.

4. Укажите основные мероприятия и процедуры профотбора, проводимыеслужбами вашей фирмы в каждом случае.

5. Опишите процедуру увольнения прежних работников и связанные с нейдействия администрации.

6. Написать тест для проверки профессиональных качеств при приеме на работу на любую одну должность.

Контрольные вопросы:

1. Какие существуют виды угроз информационным ресурсам?
2. С какой целью проводится психологический профотбор?
3. Какие структуры используются для сбора сведений о кандидатах?
4. Какие меры целесообразно предпринять до беседы с увольняемым сотрудником?
5. Какие методы используются для сбора сведений о кандидатах?
6. Что включает в себя профессиограмма?
7. Назовите тестовые приемы и другие научные методики проверки кандидатов?
8. Особенности проведения итоговой беседы с кандидатами?
9. Какие формы может принимать беседа с увольняемым сотрудником, и каким образом должен быть построен разговор?
10. Какие существуют варианты сохранения коммерческих сведений при увольнении?
11. Как рекомендуется действовать в тех случаях, когда увольнения сотрудников происходят по инициативе самих коммерческих структур?
12. Какая информация называется технологической?
13. Что включает в себя деловая информация?

Практическая работа №5 Создание и оформление графика работ и просмотр критического пути диаграмма Ганта.

Цель работы

- Закрепить теоретические знания.
- Научиться вычислять экономическую эффективность защиты информации.

Подготовка к работе

При домашней подготовке лабораторной работы необходимо подготовить отчет, содержащий:

- титульный лист с указанием варианта задания;
- цель работы;
- для выполнения работы, необходимо также изучить теоретический материал по определению экономической эффективности защиты информации, а также повторить материал, связанный с реализацией программноаппаратных и технических средств защиты информации.

Ход занятия

1. Проверка готовности студентов к работе.
2. Проверка знаний теоретического материала и алгоритма вычисления эко номической эффективности защиты информации.
3. Выполнение лабораторной работы.
4. Составление отчета.

Теоретическая часть

Основой определения эффективности защиты информации является сопоставление отношения доходов и расходов.

Экономический эффект – это конкретный результат экономической деятельности вне зависимости от затрат.

Экономическая эффективность – это результативность деятельности, соотношение доходов и расходов, а также сопоставление результатов и затрат на их достижение.

Эффективность определяется с помощью различных показателей, при этом сопоставляются данные, выражающие эффект (прибыль, объем производства, экономия от

снижения издержек) с затратами обеспечивающимиэтот эффект (капитальные вложения, текущие издержки). При решении экономических задач определяется результативность каждого предприятия и производится сопоставление различных результатов. Различают два вида экономической эффективности абсолютную и сравнительную:

абсолютную – соотношение результатов экономической деятельности и затрат для достижения этих результатов;

сравнительную – показывает изменение результатов экономической деятельности по отношению к уже достигнутым результатам;

Важное значение в расчете эффективности, в том числе и эффективности защиты информации, является приведение расчетных величин к сопоставимым значениям, которое производится до расчетов. Приведение обеспечивает точность экономических расчетов и их обоснованность. Расчеты производятся в одинаковых единицах измерения, за одинаковые отрезки времени, на одинаковое количество объектов расчета. Расчет экономического эффекта и эффективности защиты информации основывается на выявлении ущерба, нанесенного владельцу информации противоправным ее использованием, и позволяет оценить результативность защиты информации. Проведя анализ результата расчетов, можно, внести изменения в систему защиты информации для более эффективной ее защиты, т.к. разглашение данной информации влечет за собой огромные убытки (ущерб) от контрафактного ее использования злоумышленником. В ущерб входит также потерянная владельцем информации выгода вследствие противоправного использования данной информации. При расчетах данного ущерба применяются:

- ✓ Действительные цены на товары и услуги;
- ✓ Установленные законодательством нормативы платы за ресурсы;
- ✓ Установленные законодательством нормативы налогов;
- ✓ Правила и нормы расчетов физических и юридических лиц с банками;
- ✓ Ставки выплат установленных аналитическим путем для лицензионных платежей;
- ✓ Официальный курс котировки валют.

Поскольку осуществляемые затраты и получаемые результаты в течение всего срока противоправного использования информации неравноценны, то при расчетах осуществляется приведение к единому расчетному году.

Ущерб, понесенный владельцем информации из-за утраты возможности получения дохода на основе лицензионного соглашения, может быть определен исходя из размера процентных ставок, применяемых при заключении сделок, он имеет вид:

$$Упр = Ср \cdot Робщ,$$

где **Ср** – среднестатистическая ставка роялти, дается в процентах от годовой прибыли;

Общий ущерб владельца информации складывается из:

$$Р_{общ} = D_{Э} + П_{Т},$$

DЭ – ущерб владельца информации, понесенный при экспорте контрафактной продукции;

ПТ – прибыль, оставшаяся в распоряжении похитителя информации за период использования на внутреннем рынке.

Ущерб владельца информации, понесенный при экспорте контрафактнойпродукции равен произведению:

$$D_э = Z_э \cdot К_в З_э,$$

где **Z э** – валютная стоимость от экспорта продукции;

Кв курс валюты на дату расчета;

Зэ затраты на изготовление экспортной продукции;

Прибыль, оставшаяся в распоряжении похитителя информации за периодиспользования на внутреннем рынке, получается путем суммирования прибыли за каждый год периода:

$$\sum_{t}^{N \bullet t_p} (П_t * a_t),$$

где **Пt** прибыль, оставшаяся в распоряжении злоумышленника в течении года t;

at коэффициент приведения разновременных результатов.

Прибыль, оставшаяся в распоряжении злоумышленника в течении года t всвою очередь рассчитывается по формуле:

$П_t = (R_t \ C_t \ H_t)a_t$,

где Пt прибыль, оставшаяся в распоряжении прав нарушителя в течениигода t;

Rt – выручка от реализации продукции, созданной на базе противоправного использования информации в году t;

Ct – себестоимость продукции, выпущенной в году t;

Ht – общая сумма налогов и других выплат, которые были произведены в году t;

at коэффициент приведения разновременных результатов, который равен:

$at = (1+E)^{tp-t}$

tp год расчета;

E коэффициент доходности капитала;

t текущий год.

Задание:

Спрогнозировать экономическую эффективность защиты информации, полученную в 2003 году, если:

Вариант 1

E=0,1
tp=2003
t=2001
кв=30
Ср=8%
Zэ=70000$
Зэ=900000
R1=1700000 R2=2100000 R3=2500000
C1=900000 C2=1200000 C3=1500000
H1=90000 H2=130000 H3=180000

$\sum_{u} C_з \bullet$ 303000

Вариант 2

E=0,1
tp=2003
t=2001
кв=30
Ср=11%

Zэ=65000$
Зэ=820000
R1=1300000 R2=1700000 R3=2100000
C1=700000 C2=1000000 C3=1100000
H1=63000 H2=90000 H3=150000
$C_з$ ● 250000
и

Вариант 3
E=0,1
tp=2003
t=2001
кв=30
Ср=16%
Zэ=67000$
Зэ=700000
R1=2000000 R2=2050000 R3=2400000

C1=700000 C2=1000000 C3=1100000
H1=69000 H2=85000 H3=100000
$C_з$ ● 350000
и

Вариант 4
E=0,1
tp=2003
t=2001
кв=30
Ср=10%
Zэ=52000$
Зэ=680000
R1=1000000 R2=1020000 R3=1400000
C1=550000 C2=610000 C3=800000
H1=40000 H2=50000 H3=72000
$C_з$ ● 170000
и

Вариант 5
E=0,1
tp=2003
t=2001
кв=30
Ср=14%
Zэ=90000$
Зэ=700000
R1=1400000 R2=1550000 R3=1900000
C1=830000 C2=900000 C3=1000000
H1=69000 H2=76000 H3=120000
$C_з$ ● 206000
и

Контрольные вопросы:

1. Что такое экономический эффект?
2. Что называется экономической эффективностью защиты информации?
3. Какие виды экономической эффективности вы знаете, и дайте им характеристику?
4. Из чего складываются затраты на защиту информации?

Практическая работа №6 Способы обеспечения целостности данных по проекту. Ввод таблицы ресурсов и участников проекта.

Цель работы

1. Закрепить теоретические знания
2. Изучить метод расчета вероятности появления страхового случая.
3. Исследовать формирование страховых резервов.

Подготовка к работе

При подготовке к лабораторной работе необходимо подготовить отчет, содержащий:

- титульный лист с указанием варианта задания;
- цель работы;

для выполнения работы, необходимо также изучить теоретический материал по страхованию информации, расчету страхового риска и формированию страхового резерва.

Ход занятия

1. Проверка готовности студентов к работе.
2. Проверка знаний теоретического материала и порядка выполненияработы.
3. Выполнение лабораторной работы.
4. Обработка результатов.

Теоретическая часть

Отличительной чертой последних лет явилось бурное развитие информационных технологий. Уже сейчас успешность деятельности предприятия на рынке, вне зависимости от отрасли, к которой оно принадлежит, все больше зависит от его способности накапливать, эффективно обрабатывать и анализировать информацию самого различного характера. Поэтому и убытки, которые связаны с нарушением работы информационных систем (ИС) и утратой ценной информации, способны мгновенно парализовать деятельность как небольшого магазина, так и крупного промышленного предприятия. Предотвращение и ликвидация угроз информационной безопасности основывается на разработке и реализации комплекса средств и механизмов защиты. Это могут быть организационные, экономические, технические, программные, социальные, правовые и иные механизмы, обеспечивающие локализацию и предотвращение угроз.

К экономическим методам предотвращения угроз информационной безопасности можно отнести страхование, которое уменьшает финансовые потери страхователя в случае реализации риска.

Страховым риском можно назвать вероятность наступления и (или) объем ущерба (в результате оговоренного заранее события). Риск это финансовая категория. Под риском понимается возможная опасность потерь, вытекающая из специфики тех или иных явлений природы и видов деятельности человеческого общества.

Информационный риск это предполагаемое событие, ведущее к искажению, подделке, утечке, хищению, утрате информации и на случай наступления, которого проводится страхование.

Правильное и обоснованное определение страховых тарифов при защите информации исключительно важно. Владелец информационных ресурсов, в зависимости от соотношения величины тарифа и вероятности нанесения ущерба — события, от которого предусматривается введение страховой защиты, окажется в одной из трех принципиально различных ситуаций и должен принимать решение:

Случай №1, когда ущерб перекладывается в основном на страховую компанию; для страхователя владельца информационного ресурса существует конечная критическая страховая стоимость информации, при которой его риск в среднем становится нулевым. Соответственно, страхователь должен добиваться внесения в договор страхования в

качестве страховой суммы величину не меньшую, чем указанное критическое значение.

Случай №2, когда в договоре предусматривается собственное участие страхователя в покрытии части ущерба (франшиза). Это освобождает страховщика от обязанности возмещения мелких ущербов. Она выгодна для страхователя, так как обеспечивает ему льготное снижение страховых премий. *Франшиза*это определенная договором страхования сумма ущерба, не подлежащая возмещению страховщиком. Различают условную и безусловную франшизу. При *условной франшизе* страховщиком не возмещается сумма ущерба в пределах денежных средств, составляющих франшизу. Если же сумма ущерба превышает франшизу, то он возмещается полностью. При *безусловной франшизе*из любой суммы ущерба вычитается франшиза.

В третьем случае, когда ущерб перекладывается в основном на страхователя, а его риск падает пропорционально увеличению размера страховой стоимости информации.

Обобщенная модель риска основывается на функциональных зависимостях между стоимостью *S* страхования, вероятностью преодоления системы защиты информации P, а следовательно и размером возникающего при этом ущерба *U*.

Уточним следующие величины:

P_i^{**} -вероятность наступления страхового случая при возникновении i-ой угрозы;

P_i^{*} – вероятность появления i$^{-ой}$ угрозы;

p_i – предполагаемая вероятность преодоления системы защиты i$^{-ой}$ угрозой; m_i – количество успешных попыток преодоления системы защиты i$^{-ой}$ угрозой;

m_{0i} – предполагаемое количество успешных попыток преодоления системызащиты i$^{-ой}$ угрозой;

n_i – общее количество попыток преодоления системы защит i$^{-ой}$ угрозой;

S – стоимость страхования от i$^{-ой}$ угрозы;

a,b,c коэффициенты пропорциональности интервалы стоимости страхования (не является непрерывной величиной).

Типичная зависимость уровня риска от стоимости страхования, полученная при условии того, что вероятность нанесения ущерба P(S) уменьшается с ростом стоимости S приведена на рис. 1. При некоторой стоимости s_2 риск имеет наименьшее значение. Эта стоимость является оптимальной. Дальнейший, сверх оптимального значения, рост затрат на страхование будет вести к увеличению экономических потерь собственника информации

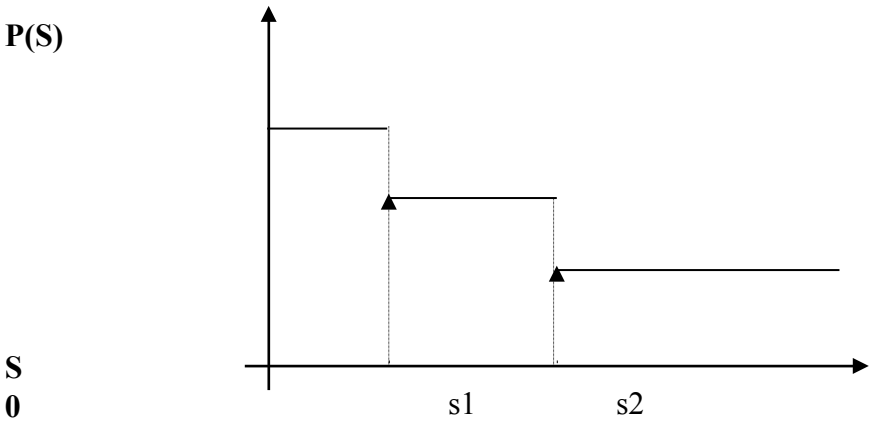

Рис. 1. Зависимость уровня риска от стоимости страхования.

Если владелец информационных ресурсов, не проводит тщательного анализа и не оптимизирует размер выделяемых на страхование средств, практически всегда оказывается в экономическом проигрыше. Эффективностьэтого метода во многом зависит от точности определения страховой стоимости защищаемых информационных ресурсов, а

также степени соответствия тарифной ставки вероятности несанкционированных действий. Реализации страхования информации мешает проблема отсутствия достаточно точных практических методик по определению ее стоимости и обоснованию тарифов.

Формирование страховых резервов.

Страховые резервы это конкретная величина обязательств страховщика по всем заключенным со страхователями договорам, не исполненных на какую-либо отчетную дату.

Резервы страховых организаций рассматриваются отдельно по страхованию жизни и по страхованию иному, чем страхование жизни. Нас в данном случае интересует страхование иное, чем страхование жизни.

Расчет резервов по страхованию иному, чем страхование жизни

Правила формирования страховых резервов по страхованию иному, чем страхование жизни, утверждены приказом Министерства финансов РФ от 11 июня 2002 г. № 51Н. Страховщики руководствуются этими Правилами и на их основе разрабатывают и утверждают Положение о формировании страховых резервов по указанным видам страхования и представляют их в Министерство финансов РФ в течение месяца с момента утверждения.

Страховые резервы включают:

- резерв не заработанной премии (РНГГ);
- резервы убытков:
  - ✓ резерв заявленных, но неурегулированных убытков (РЗУ),
  - ✓ резерв происшедших, но незаявленных убытков (РПНУ);
- стабилизационный резерв (СР);
- иные страховые резервы.

Для расчета страховых резервов договоры распределяются по следующимучетным группам:

Учетная группа 1. Страхование (сострахование) от несчастных случаев и болезней.
Учетная группа 2. Добровольное медицинское страхование (сострахование). Учетная группа 3. Страхование (сострахование) информационных ресурсов. Учетная группа 4. Страхование (сострахование) граждан, выезжавших за рубеж.
Учетная группа 5. Страхование (сострахование) средств наземного транспорта.
Учетная группа 6. Страхование (сострахование) средств воздушного транспорта.
Учетная группа 7. Страхование (сострахование) средств водного транспорта.
Учетная группа 8. Страхование (сострахование) грузов.
Учетная группа 9. Страхование (сострахование) товаров на складе.
Учетная группа 10. Страхование (сострахование) средств обработки информации.
Учетная группа 11. Страхование (сострахование) предпринимательских (финансовых) рисков.
Учетная группа 12. Страхование (сострахование) имущества, кроме перечисленного в учетных группах 1-11.
Учетная группа 13. Страхование (сострахование) профессиональной ответственности.
Учетная группа 14. Страхование (сострахование) ответственности за неисполнение обязательств.

Расчет резерва незаработанной премии.

Резерв не заработанной премии (РНП) это часть начисленной страховойпремии по договору, относящаяся к периоду действия договора, выходящему за пределы отчетного

периода (незаработанная премия, предназначенная для исполнения обязательств по обеспечению предстоящих выплат, которые могут возникнуть в следующих отчетных периодах).

Расчет РНП производится отдельно по каждой учетной группе. Величина РНП определяется путем суммирования резервов незаработанной премии по

всем учетным группам договоров. Для расчета незаработанной премии (НП)по каждому договору определяется базовая страховая премия (БСП).

БСП = страховой брутто-премии минус начисленные вознаграждения за заключенные договора страхования (со страхования) и минус отчисления от страховой брутто-премии в случаях, предусмотренных действующим законодательством.

Для расчета не заработанной премии НП по договору (договорам), принятому в перестрахование, используют следующие методы:

- *«pro rata temporize»*;
- «одной двадцать четвертой» (далее «1/24»);
- «одной восьмой» (далее «1/8»).

Незаработанная премия методом *«pro rata temporis»* определяется по каждому договору как произведение базовой страховой премии по договору на отношение не истекшего на отчетную дату срока действия договора (в днях) ко всему сроку действия договора (в днях):

$$НП_i = БСП_i \bullet \frac{n_i - m_i}{n_i},$$

где: БСПi – базовая страховая премия по іму договору;

ni – срок действия договора в днях;

mi –число дней с момента вступления і-го договора в силу до отчетнойдаты.

Резерв незаработанной премии равен сумме НПi , исчисленной по каждому договору страхования.

Расчет резерва незаработанной премии методом «1/24»

Для расчета незаработанной премии методом «1/24» договоры, относящиеся к одной учетной группе, группируют по подгруппам. В подгруппу включаются договоры с одинаковыми сроками действия (в месяцах) и с датами начала их действия, приходящимися на одинаковые месяцы.

Для расчета НП методом «1/24» принимается, что:

1) дата начала действия договора приходится на середину месяца;

2) срок действия договора, не равный целому числу месяцев, равен ближайшему большему числу месяцев.

Таким образом не заработанная премия по каждой подгруппе имеет вид:

*НПi=БСПi*Коэффициент для расчета величины резерва НП,*

где: НПi – незаработанная премия по і-ой подгруппе;

БСПi – базовая страховая премия по i-му договору.

Коэффициент для каждой подгруппы определяется как отношение не истекшего на отчетную дату срока действия договора подгруппы (в половинах месяцев) ко всему сроку действия договоров подгруппы (в половинах месяцев).

Резерв не аработанной премии методом «1/24» в целом по учетной группе определяется путем суммирования не заработанных премий, рассчитанных по каждой группе.

Расчет резерва незаработанной премии методом «1/8»

Для расчета незаработанной премии методом «1/8» договоры, относящиеся к одной учетной группе, группируют по подгруппам. В подгруппу включаются договоры с одинаковыми сроками действия (в кварталах) и с датами начала их действия, приходящимися на одинаковые кварталы.

Для расчета НП методом «1/8» принимается, что:

1) дата начала действия договора приходится на середину квартала;
2) срок действия договора, не равный целому числу кварталов, равен ближайшему большему числу кварталов.

Таким образом не заработанная премия по каждой подгруппе имеет вид: *НПi=БСПi*Коэффициент для расчета величины резерва НП,* где: НПi – незаработанная премия по i-ой подгруппе; БСПi – базовая страховая премия по i-му договору.

Коэффициент для каждой подгруппы определяется как отношение не истекшего на отчетную дату срока действия договора подгруппы (в половинах кварталов) ко всему сроку действия договоров подгруппы (в половинах кварталов).

Резерв незаработанной премии методом «1/24» в целом по учетной группе определяется путем суммирования не заработанных премий, рассчитанных по каждой группе.

Задание.

Вариант №1

1. Базовая страховая премия по подгруппам договоров, относящихся к учетной группе 3 (страхование информационных ресурсов), заключенных сроком на 1 год, составила по кварталам прошедшего года (тыс. руб.):

в первом – 260 во втором – 320в третьем – 480

в четвертом – 380.

Определите резерв незаработанной премии на 1 января методом «1/8».

2. Базовая страховая премия по подгруппам договоров, относящихся к учетной группе 10 (страхование средств обработки информации) и заключенных сроком на 1 год в прошедшем году составила:

в январе -70,

в июне – 120,

в декабре – 50.

Определите резерв незаработанной премии методом «1/24» на 1 января.

3. Страховой компанией заключен договор страхования систем бесперебойного питания на период с 1 февраля по 31 августа. Страховая сумма 3600 тыс. руб., страховой тариф 2%. Вознаграждение агенту за заключение договора 10%, отчисления в резерв предупредительных мероприятий 2%. Рассчитайте величину незаработанной премии на 1 июля по данному договору методом *«pro rata temporis».*

Вариант №2.

1. Базовая страховая премия по подгруппам договоров, относящихся к учетной группе 3 (страхование информационных ресурсов), заключенным сроком на 1 год, составила по кварталам прошедшего года (тыс. руб.):
в первом – 80 во втором – 120в третьем – 210
в четвертом – 180.
Определите резерв незаработанной премии на 1 января методом «1/8».

2. Базовая страховая премия по подгруппам договоров, относящихся к учетной группе 3 (страхование информационных ресурсов), заключенных сроком на 1 год в прошедшем году (тыс. руб.):
в феврале 180,
в июле 270,
в ноябре 490.
Определите резерв незаработанной премии на 1 января методом «1/24».

3. Страховой компанией заключен договор страхования систем хранения информации на период с 1 марта по 31 июля текущего года. Страховая брутто премия 50 тыс. рублей. Комиссионное вознаграждение 10%, отчисленияв резерв предупредительных мероприятий 3%.
Определите величину незаработанной премии на 1 июля по данному договору методом *«pro rata temporis».*

Вариант №3.

1. Базовая страховая премия по подгруппам договоров, относящихся к учетной группе 3 (страхование информационных ресурсов), заключенных сроком на 1 год, составила по кварталам прошедшего года (тыс. руб.):
в первом – 110
во втором – 250
в третьем – 320
в четвертом – 380.
Определите резерв незаработанной премии на 1 января методом «1/8».

2. Базовая страховая премия по подгруппам договоров, относящихся к учетной группе 10 (страхование средств обработки информации), заключенных сроком на 1 год в прошедшем году (тыс. руб.):
в марте 200,
в августе 290,
в октябре 320.
Определите резерв незаработанной премии на 1 января методом «1/24».

3. Страховой компанией 1 августа заключен договор страхования программно-аппаратной информационной системы на срок до 1 мая следующего года. Страховая брутто премия –120 тыс. рублей. Вознаграждение агенту за заключение договора страхования – 7%, отчисления в резерв предупредительных мероприятий-3%. Определите незаработанную премию на 1 января по данному договору страхования.

Вариант №4.

1. Определите резерв незаработанной премии на 1 октября по двум договорам методом *«pro rata temporis».* Срок действия договора страхования имущества телекоммуникационных систем с 1 февраля по 1 декабря текущего года, страховая премия по данному договору составила 220 тыс. руб. Срок действия договора добровольного

страхования финансового риска непогашения кредита с 1 июня по 1 ноября. Страховая премия по данному договору страхования составила 12 тыс. руб. Вознаграждение, выплаченное за заключение первого договора, -6,8 тыс. руб., второго 0,4 тыс. руб. Отчисления на финансирование предупредительных мероприятий по первому договору 3,5 тыс. руб., по второму 0,6 тыс. руб.

2. Рассчитать вероятность появления страхового случая при заданных значениях. Построить график зависимости уровня риска (вероятность наступления страхового случая) от стоимости страхования. Значения, заданных параметров находятся в таблице №1.

Таблица 1.

Угрозы	m_{0i}	n_i	S (тыс. руб)	s1 (тыс. руб)	s2 (тыс. руб)	a	b	c
1	253	515	500	300	600	-10	5	15
2	112	200	200	300	600	-10	5	15
3	575	1115	700	300	600	-10	5	15
4	413	801	600	300	600	-10	5	15
5	170	3	462	300	600	-10	5	15

Вариант №5

1. Определите резерв незаработанной премии на 1 июля по двум договорам методом *«pro rata temporis»*. Срок действия договора страхования систембесперебойного питания с 10 февраля по 10 ноября текущего года; страховая премия по данному договору составила 50 тыс. руб. Срок действия договора страхования риска выхода из строя системы кондиционирования воздуха с 1 марта по 1 декабря текущего года; страховая премия по данному договору составила 80 тыс. руб. Вознаграждение, выплаченное за заключение первого договора, 5 тыс. руб., второго 8 тыс. руб. Отчисления на финансирование предупредительных мероприятий по каждому договору -2,5 тыс. руб.

2. Рассчитать вероятность появления страхового случая при заданных значениях. Построить график зависимости уровня риска (вероятность наступления страхового случая) от стоимости страхования. Значения, заданных параметров находятся в таблице №2.

Таблица 2.

Угрозы	m_{0i}	n_i	S (тыс. руб)	s1 (тыс. руб)	s2 (тыс. руб)	a	b	c
1	100	173	230	300	600	-10	5	15
2	328	659	400	300	600	-10	5	15
3	211	461	600	300	600	-10	5	15
4	230	426	750	300	600	-10	5	15
5	95	164	100	300	600	-10	5	15

Контрольные вопросы

1. Что называется страховым риском?
2. Что понимается под информационным риском?
3. Франшиза и ее виды?
4. Что понимается под страховыми резервами?
5. Что включают в себя страховые резервы?
6. Что называется резервом не заработанной премии?
7. Чему равняется базовая страховая премия?

Практическая работа №7. Решение проблемы перегрузки ресурсов по проекту информационной безопасности. Способы оптимизации графика работ

Цель работы

1. Закрепить теоретические знания
2. Изучить метод совокупной стоимости владения Total Cost of Ownership (TCO)

3.Изучить методику Return on Investment for Security (расчет возврата инвестиций в безопасность)

Теоретическая часть

Совокупная стоимость владения Total Cost of Ownership (TCO)

Анализ методов оценки эффективности инвестиций в корпоративные системы информационной безопасности показывает, что только метод совокупной стоимости владения в явном виде позволяет рассчитать расходную часть на систему безопасности. Поэтому на сегодняшнем практическом занятии рассмотрим методику ССВ более подроб но.

Совокупная стоимость владения (Total Cost of Ownership) первоначально разрабатывалась как средство расчета стоимости владения компьютером. Но в последнее время благодаря усилиям компании Gartner Group эта методика стала основным инструментом подсчета совокупной стоимости владения корпоративных систем защиты информации. Основной целью расчета ССВ является выявление избыточных статей расхода и оценка возможности возврата инвестиций, вложенных в технологии безопасности. Таким образом, полученные данные по совокупной стоимости владения используются для выявления расходной части использования корпоративной системы защиты информации.

Главной проблемой при определении ССВ является проблема выявления составляющих совокупной стоимости владения и их количественная оценка. Все составляющие ССВ условное разделяются на «видимые» пользователю (первоначальные затраты) и «невидимые» (затраты на эксплуатацию и использование). При этом «видимая» часть ССВ составляет 32%, а по некоторым оценкам и 21 %, а «невидимая» — 68 % или соответственно79 %.

К группе «видимых» затрат относятся следующие:

- стоимость лицензии;
- стоимость внедрения;
- стоимость обновления;
- стоимость сопровождения.

Все эти затраты, за исключением внедрения, имеют фиксированную стоимость и могут быть определены еще до принятия решения о внедрении корпоративной системы защиты информации. Следует отметить, что и в «видимом» секторе поставщиками систем безопасности иногда могут использоваться скрытые механизмы увеличения стоимости для привлечения клиента.

Дополнительные затраты («невидимые») появляются у каждого предприятия, завершившего у себя внедрение корпоративной системы защиты информации. «Невидимые» затраты также разделяются на группы:

- затраты на оборудование (включают в себя затраты на приобретение или обновление средств защиты информации, на организацию бесперебойного питания и резервного копирования информации, на установку новых устройств безопасности и пр.);
- дополнительное программное обеспечение (системы управления безопасностью, VPN, межсетевые экраны, антивирусы и пр.);
- персонал (например, ошибки и трудности в работе со средствами защиты, неприятие или даже саботаж новых средств защиты и т. д.);

• стоимость возможностей стоимость возможных альтернатив (приобретение или обновление корпоративной системы защиты информации/сделать это собственными силами или заказать у сторонней организации);

• другие (в этом случае оценивается степень и стоимость риска «выхода из строя» системы).

Показатель ССВ корпоративной системы информационной безопасности рассчитывается как сумма всех затрат, «видимых» и «невидимых». Затем этот показатель сравнивается с рекомендуемыми величинами для данного типа предприятия. Существует 17 типов предприятий, которые, в свою очередь, делятся на малые, средние и крупные.

Если полученная совокупная стоимость владения системы безопасности значительно превышает рекомендованное значение и приближается к предельному, то необходимо принять меры по снижению ССВ. Сокращения совокупной стоимости владения можно достичь следующими способами: максимальной централизацией управления безопасностью, уменьшением числа специализированных элементов, настройкой прикладного программного обеспечения безопасности и пр.

Основные положения методики Total Cost of Ownership

Совокупная стоимость владения (показатель ТСО) для системы информационной безопасности в общем случае складывается из стоимости:

• проектных работ;

• закупки и настройки программно-технических средств защиты, включающих следующие основные группы: межсетевые экраны, средства криптографии, антивирусы и средства аутентификации, авторизации и администрирования (AAA);

• затрат на обеспечение физической безопасности;

• обучения персонала;

• управления и поддержки системы (администрирование безопасности);

• аудита информационной безопасности;

• периодической модернизации системы информационной безопасности.

Таким образом, методика совокупной стоимости владения компании Gartner Group позволяет:

• получить адекватную информацию об уровне защищенности распределенной вычислительной среды и совокупной стоимости владения корпоративной системы защиты информации;

• сравнить подразделения службы информационной безопасности компании, как между собой, так и с аналогичными подразделениями других предприятий в данной отрасли;

• оптимизировать инвестиции на ИБ компании с учетом реального значения показателя совокупной стоимости владения.

Здесь под показателем совокупной стоимости владения понимается сумма прямых и косвенных затрат на организацию (реорганизацию), эксплуатацию и сопровождение корпоративной системы защиты информации в течение года. ССВ может рассматриваться как ключевой количественный показатель эффективности организации ИБ в компании, так как позволяет не только оценить совокупные затраты на ИБ, но управлять этими затратами для достижения требуемого уровня защищенности КИС.

При этом прямые затраты включают как капитальные компоненты затрат (ассоциируемые с фиксированными активами или «собственностью»), так и трудозатраты, которые учитываются в категориях операций и административного управления. Сюда же относят затраты на услуги удаленных пользователей, аутсортинг и др., связанные с поддержкой деятельности организации.

В свою очередь, косвенные затраты отражают влияние КИС и подсистемы защиты информации на сотрудников компании посредством таких измеримых показателей, как простои и «зависания» корпоративной системы защиты информации и КИС в целом, затраты на операции и поддержку (не относящиеся к прямым затратам).

Очень часто косвенные затраты играют значительную роль, так как они обычно изначально не отражаются в бюджете на ИБ, а выявляются явно при анализе затрат впоследствии, что в конечном счете приводит к росту «скрытых» затрат компании на систему информационной безопасности.

Существенно, что ССВ не только отражает «стоимость владения» отдельных элементов и связей корпоративной системы защиты информации в течение их жизненного цикла. «Овладение методикой» ТСО помогает службе ИБ лучше измерять, управлять и снижать затраты и/или улучшать уровни сервиса защиты информации с целью адекватности мер защиты бизнесу компании.

Подход к оценке ТСО базируется на результатах аудита структуры и поведения корпоративной системы защиты информации и КИС в целом, включая действия сотрудников служб автоматизации, информационной безопасности и просто пользователей КИС. Сбор и анализ статистики по структуре прямых (HW/SW, операции, административное управление) и косвенных затрат (на конечных пользователей и простои) проводится, как правило, в течение 12 месяцев. Полученные данные оцениваются по ряду критериев с учетом сравнения с аналогичными компаниями по отрасли.

Методика ССВ(ТСО) позволяет оценить и сравнить состояние защищенности КИС компании с типовым профилем защиты, в том числе показать узкие места в организации защиты, на которые следует обратить внимание. Иными словами, на основе полученных данных можно сформировать понятную с экономической точки зрения стратегию и тактику развития корпоративной системы защиты информации, а именно:

«сейчас мы тратим на ИБ столько-то, если будем тратить столько-то по конкретным направлениям ИБ, то получим такой-то эффект».

Известно, что в методике ССВ(ТСО) в качестве базы для сравнения используются данные и показатели ССВ для западных компаний. Однако данная методика способна учитывать специфику российских компаний с помощью так называемых поправочных коэффициентов, например:

- по стоимости основных компонентов корпоративной системы защиты информации и КИС, информационных активов компании (Cost Profiles) с учетом данных по количеству и типам серверов, персональных компьютеров, периферии и сетевого оборудования;
- по заработанной плате сотрудников (Salary and Asset Scalars) с учетом дохода компании, географического положения, типа производства и размещения организации в крупном городе или нет;
- по конечным пользователям ИТ (End User Scalars) с учетом типов пользователей и их размещения (для каждого типа пользователей требуется различная организация службы поддержки и вычислительной инфраструктуры);
- по использованию методов так называемой лучшей практики в области управления ИБ (Best Practices) с учетом реального со стояния дел по управлению изменениями, операциями, активами, сервисному обслуживанию, обучению, планированию и управлению процессами; по уровню сложности организации (Complexity Level) с учетом состояния организации конечных пользователей (процент влияния 40 %), технологии SW (40 %), технологии HW (20 %).

В целом, определение затрат компании на ИБ подразумевает решение следующих трех задач:

- оценку текущего уровня ТСО корпоративной системы защиты информации и КИС в целом;
- аудит ИБ компании на основе сравнения уровня защищенности компании и рекомендуемого (лучшая мировая практика) уровня ТСО;
- формирование целевой модели ТСО. Рассмотрим каждую из перечисленных задач.1. Оценка текущего уровня ТСО

В ходе работ по оценке ТСО проводится сбор информации и расчет показателей ТСО организации по следующим направлениям:

- существующие компоненты ИС (включая систему защиты информации) и информационные активы компании (серверы, клиентские компьютеры, периферийные устройства, сетевые устройства);
- существующие расходы на аппаратные и программные средства защиты ин формации (расходные материалы, амортизация);
- существующие расходы на организацию ИБ в компании (обслуживание СЗИ и СКЗИ, а также штатных средств защиты периферийных устройств, серверов, сетевых устройств, планирование и управление процессами защиты информации, разработка концепции и политики безопасности и пр.);
- существующие расходы на организационные меры защиты информации;
- существующие косвенные расходы на организацию ИБ в компании и, в частности, обеспечение непрерывности или устойчивости бизнеса компании.

2. Аудит информационной безопасности компании

По результатам собеседования с TOP-менеджерами компании и проведения инструментальных проверок уровня защищенности организации проводится анализ следующих основных аспектов:

- политики безопасности;
- организации защиты;
- классификации и управления информационными ресурсами;
- управления персоналом;
- физической безопасности;
- администрирования компьютерных систем и сетей;
- управления доступом к системам;
- разработки и сопровождения систем;
- планирования бесперебойной работы организации;
- проверки системы на соответствие требованиям ИБ.

На основе проведенного анализа выбирается модель ТСО, сравнимая со средними и оптимальными значениями для репрезентативной группы аналогичных организаций, имеющих схожие с рассматриваемой организацией показатели по объему бизнеса. Такая группа выбирается из банка данных по эффективности затрат на ИБ и эффективности соответствующих профилей защиты аналогичных компаний.

Сравнение текущего показателя ТСО проверяемой компании с модельным значением показателя ТСО позволяет провести анализ эффективности организации ИБ компании, результатом которого является определение «узких» мест в организации, причин их появления и выработка дальнейших шагов по реорганизации корпоративной системы защиты информации и обеспечения требуемого уровня защищенности КИС.

3. Формирование целевой модели ТСО

По результатам проведенного аудита моделируется целевая (желаемая) модель, учитывающая перспективы развития бизнеса и корпоративной системы защиты информации (активы, сложность, методы лучшей практики, типы СЗИ и СКЗИ, квалификация сотрудников компании и т. п.).

Кроме того, рассматриваются капитальные расходы и трудозатраты, необходимые для проведения преобразований текущей среды в целевую среду. В трудозатраты на внедрение включаются затраты на планирование, развертывание, обучение и разработку. Сюдаже входят возможные временные увеличения затрат на управление и поддержку.

Для обоснования эффекта от внедрения новой корпоративной системы защиты информации (ROSI) могут быть использованы модельные характеристики снижения совокупных затрат (ТСО), отражающие возможные изменения в корпоративной системе защиты информации.

Пример использования методики Total Cost of Ownership

Пусть объектом исследования является страховая компания ЗАО «Страхование». Для определения затрат на систему информационной безопасности по методике совокупной стоимости владения воспользуемся программным продуктом «TCO Manager» компании Gartner Group. Технология работы с ПП «TCO Manager» заключается в следующем: пользователь вводит первоначальные данные об объекте (профайл компании, данные о конечных пользователях, об информационных активах предприятия), исходя из них, определяется текущий показатель ССВ (TCO) и вычисляются ежегодные затраты на поддержание существующего уровня безопасности. Также «TCO Manager» позволяет оптимизировать показатель TCO, сравнив текущий показатель TCO компании с «лучшим» в отрасли и смоделировав целевой показатель TCO для данного предприятия.

Обратимся к исходным данным по ЗАО «Страхование», представленным в таблице1 и вычислим текущий показатель TCO.

Табл.1. Исходные данные ЗАО «Страхование»

Название компании	ЗАО «Страхование»
Период анализа	январь-декабрь 2004
Основной вид деятельности	Страхование
Общий годовой доход	450 млн. рублей
Количество рабочих часов в год	1880 ч/год
Средняя годовая зарплата конечных пользователей	38000 рублей
Средний процент, отчисляемый на налоги, медицинское страхование, страхование от несчастных случаев и т. д., персонала службы безопасности (ECH):	37 %
Средний процент, отчисляемый на налоги, медицинское страхование, страхование от несчастных случаев и т. д., конечных пользователей (ECH):	37 %
Количество конечныхпользователей:	2869 чел.

Классификация конечных пользователей, а также текущие затраты на сетевое оборудование представлены в таблицах 2,3 и 4.

Табл.2. Классификация конечных пользователей по типам

Тип конечных пользователей	**В процентном соотношении, %**	**Количество человек**
Руководящий персонал	1	29
Научные работники	20	574
Исполнительный персонал	75	2152
Операторы	4	115
Общее количество	100	2869

Табл.3. Классификация конечных пользователей по мебстоположению

Тип местоположения	**В процентном соотношении, %**	**Количество человек**
Стационарное	85	2439
Мобильное	10	287
Телекоммуникационное	5	143
Общее колличество	100	2869

Табл.4. Текущие затраты на сетевое оборудование

Сетевое оборудование	**Текущие затраты, тыс. руб.**
Servers	90
Client-Desktor	2810
Client-Mobile	350
Peripherals	617
Network Device Assets	212
Total Assets	4079

Форма ввода данных «Интервью» в «TCO Manager» содержит сведения об информационных активах предприятия (аппаратные средства и программное обеспечение), информацию о конечных пользователях, и на основании этих данных мы получаем следующие отчеты (табл. 6-8). Также «TCO Manager», используя практический подход к определению совокупной стоимости владения, позволяет сравнивать текущие затраты с эталонными («лучшими в группе») и строить целевые показатели затрат. В частности в табл. 716 приведена детализация и расшифровка укрупненных прямых и косвенных затрат, которые отображены в табл.6. Целевые показатели являются моделируемыми на основании проекта модернизации корпоративной системы антивирусной защиты и системы управления доступом на объекте информатизации (физической защиты).

Условно определяют три возможных состояния системы защиты КИС от вирусов и вредоносного программного обеспечения, а именно: базовое, среднее и высокое. Рассмотрим характеристики этих состояний.

Базовое. Стационарные и мобильные рабочие станции обладают локальной защитой от вирусов. Антивирусное программное обеспечение и базы сигнатур регулярно обновляются для успешного распознавания и парирования новых вирусов. Установлена программа автоматического уничтожения наиболее опасных вирусов. Основная цель уровня организация минимальной защиты от вирусов и враждебного программного обеспечения при небольших затратах.

Среднее. Установлена сетевая программа обнаружения вирусов. Управление программными обновлениями на сервере автоматизировано. Системный контроль над событиями оповещает о случаях появления вирусов и предоставляет информацию по предотвращению дальнейшего распространения вирусов. Превентивная защита от вирусов предполагает выработку и следование определенной политики защиты информации, передаваемой по открытым каналам связи Интернета. Дополнительно к техническим мерам активно предлагаются и используются организационные меры защиты информации.

Высокое. Антивирусная защита воспринимается как один из основных компонентов корпоративной системы защиты. Система антивирусной защиты тесно интегрирована в комплексную систему централизованного управления ИБ компании и обладает максимальной степенью автоматизации. При этом организационные меры по защите информации преобладают над техническими мерами. Стратегия защиты информации определяетсяисключительно стратегией развития бизнеса компании.

Согласно практическому подходу (best practice) в «TCO Manager» формируется отчет (табл. 5) для ЗАО «Страхование», в котором отражаются требования к состоянию корпоративной системы защиты на основании данных о типе предприятия и текущего показателя TCO.

Табл. 5. ***Сравнение текущего и целевого состояния системы защиты***

Критерии	Текущий уровень	Целевой уровень
Усовершенствование технологии управления активами		
Автоматизированное управление активами	Базовый	Высокий
Учет программного обеспечения	Базовый	Высокий
Учет аппаратных средств	Базовый	Высокий
Усовершенствование технологии управления системы		
Системы обнаружения вирусов и защиты	Базовый	Высокий
Системное управление	Базовый	Средний
Стандартизация процессов модернизации		
Стандартизация поставщиков	Базовый	Средний
Стандартизация платформы	Средний	Высокий
Совершенствование управления персоналом		
Обучение пользователей	Базовый	Высокий
Обучение ИТ-специалистов	Базовый	Средний
Мотивация ИТ-персонала	Базовый	Средний
Организация устойчивой ИТ-службы	Базовый	Средний

Табл 6. ***Анализ затрат по показателям ТСО***

Категории затрат	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Прямые затраты									
Затраты на программное обеспечение и оборудование	5 601 557	4 931 610	5 400 695	–669 947	–12	469 085	10	200 862	–4
Операционные затраты (управление)	4 831 911	4 711 401	2 695 527	–120 511	–2	–2 015 873	–43	–2 136 384	–44
Административные затраты (поддержка)	1 477 957	994 636	1 272 225	–483 321	–33	277 589	28	–205 732	–14
Общие прямые	**11 911 426**	**10 637 647**	**9 368 447**	**–173 779**	**–11**	**–1 269 199**	**–12**	**–2 542 978**	**–21**
Косвенные затраты									
Поддержка конечных пользователей	11 853 266	20 458 366	9 005 139	8 605 100	73	–11 453 227	–56	–2 848 127	–24
Простой	2 619 053	636 117	1 491 347	–1 982 936	–76	855 230	134	–1 127 705	–43
Общие косвенные	**14 472 318**	**21 094 483**	**10 496 486**	**6 622 165**	**46**	**–10 597 997**	**–50**	**–3 975 832**	**–27**
Ежегодный ТСО	26 383 744	31 732 130	19 864 933	5 348 386	20	–11 867 196	–37	–6 518 811	–25
Процент ТСО от дохода	59	71	44	12	203	–26	–374	–14	–247
Процент прямых затрат от дохода	26	24	21	–03	–107	–03	–119	–06	–213

Таким образом, можно сделать вывод о том, что ЗАО «Страхование» необходимо повышать уровень защиты информационной системы от вирусов, совершенствовать технологию управления активами и проводить обучение конечных пользователей и специалистов отдела информационных технологий.

Теперь обратимся к отчетам по совокупной стоимости владения, приведенных в таблицах, и проанализируем полученные показатели ТСО.

Сопоставляя результаты сравнения в табл. 5 и данные отчетов (см. табл. 6-16), можно сделать следующие выводы: при построении целевой модели ТСО наибольшему снижению подверглись административные затраты на управление (на 44 %) и затраты при простое (на 43 %). Сокращение административных расходов связано, в основном, с внедрением автоматизированной системы управления активами, а значительное снижение затрат от простоев с пересмотром уровня знаний конечных пользователей и ИТ-персонала

и увеличением затрат на обучение.

Небольшое повышение затрат на аппаратные средства (на 16%) вызвано закупкой оборудования, необходимого для внедрения корпоративной системы защиты.

Таким образом, целевой показатель ТСО значительно меньше текущего, но вместе с тем поддержание соответствующего уровня защиты требует существенных расходов (57% от ежегодного дохода), и для обоснования этих расходов необходимо применять методы оценки эффективности инвестиций в корпоративную систему информационной безопасности.

Табл. 7. Детализация затрат на программное обеспечение и оборудование по категориям

Категории затрат на программное обеспечение и оборудование	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Оборудование	2 451 546	2 617140	2 836 522	165 594	7	219 382	8	384 976	16
Программное обеспечение	2 873 154	2 040 780	2 262 723	–832 374	–29	221 943	11	–610 431	–21
Оборудование ИС	79617	78 690	89 665	–927	–1	10 975	14	10 048	13
Программное обеспечение ИС	197 240	195 000	211 786	–2240	–1	16 786	9	14 546	7
Общие затраты	**5 601 557**	**4 931 610**	**5 400 695**	**–669 947**	**–12**	**469 085**	**10**	**–200 862**	**–4**

*Табл. 8. **Расшифровка затрат на аппаратные средства***

Категории затрат на аппаратные средства	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Покупка оборудования	1 909 668	1 894 950	2 109 357	–14 718	–1	214 407	11	199 689	10
Лизинговые платежи	307 521	260 480	395 994	–47 041	–15	135 514	52	88 473	29
Модернизация	67 972	258 340	57 254	190 368	280	–201 086	–78	–10 717	–16
Комплектующие	81 855	36 640	165 148	–45 215	–55	128 508	351	83 292	102
Лицензии	84 530	166 730	108 769	82 200	97	–57 961	–35	24 238	29
Общие затраты	**2 451 546**	**2 617 140**	**2 836 522**	**165 594**	**7**	**219 382**	**8**	**384 976**	**16**

*Табл. 9. **Расшифровка затрат на программное обеспечение***

Категории затрат на программное обеспечение	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Затраты на собственную разработку программных продуктов и баз данных	502 767	352 500	427 128	–150 267	–30	74 628	21	–75 639	–15
Затраты на бизнес-приложения и инженерное программное обеспечение	1179 383	1 393 000	1 002 000	213 617	18	-391 000	–28	–177 382	–15
Затраты на средства и инструменты разработки	410 817	57 480	357 167	–353 337	–89	299 687	521	–53 650	–13
Затраты на формирование системы внутренних коммуникаций	163 804	49 400	142 425	–114 404	–70	93 025	188	–21 379	–13
Другие	616 384	188 400	334 003	–427 984	–69	145 603	77	–282 381	–46
Общие затраты	**2 873 154**	**2 040 780**	**2 262 723**	**–832 374**	**–29**	**221 943**	**11**	**–610 431**	**–21**

Табл 10. ***Детализация операционных затрат***

Операционные затраты	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Обслуживание клиентских мест и периферийных устройств	1 563 387	2 473 600	836 474	910 213	58	–1 637 126	–66	–726 913	–46
Обслуживание серверов	559 468	427 961	336 049	–131 507	–24	–91 912	–21	–223 419	–40
Обслуживание сети	223 624	253 680	171 567	30 056	13	–82 113	–32	–52 056	–23
Планирование и управление процессами	460 701	0	329 119	–460 701	–100	329 119	Undefined	–131 582	–29
Обслуживание и администрирование баз данных	241 331	0	230 757	–241 331	–100	230 757	Undefined	–10 574	–4
Затраты на сервисную поддержку	1 783 400	1 556 160	791 561	–227 240	–13	–764 599	–49	–991 839	–56
Общие ежегодные затраты	**4 831 911**	**4 711 401**	**2 695 527**	**–120 511**	**–2**	**–2 015 873**	**–43**	**–2 136 384**	**–44**

Табл. 14. ***Детализация административных затрат***

Административные затраты	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Финансовые и административные затраты	795 837	665 036	575 326	–130 801	–16	–89 710	–13	–220 511	–28
Затраты на обучение ИТ-специалистов	188 798	114 240	188 339	–74 558	–39	74 099	65	–459	0
Обучение конечных пользователей	493 322	215 360	508 560	–277 962	–56	293 200	136	15 237	3
Общие ежегодные	**1 477 957**	**994 636**	**1 272 225**	**–483 321**	**–33**	**277 589**	**28**	**–205 732**	**–14**

Табл. 11. ***Расшифровка затрат на обслуживание клиентских мест и периферийных устройств***

Затраты на обслуживание клиентских мест и периферийных устройств	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Решение проблем 2 уровня	247 995	494 720	121 749	246 725	99	–372 971	–75	–126 246	–51
Решение проблем 3 уровня	86 580	296 832	32 519	210 252	243	–264 313	–89	–54 061	–62
Планирование и управление трафиком	32 449	123 680	30 753	91 231	281	–92 927	–75	–1696	–5
Точная настройка	24 337	74 208	22 871	49 871	205	–51 337	–69	–1466	–6
Администрирование конечных пользователей	62 903	296 832	33 507	233 929	372	–263 325	–89	–29 396	–47
Поддержка операционной системы	50 821	74 208	23 106	23 387	46	–51102	–69	–27 715	–55
Обслуживание рабочей силы	105 663	123 680	72 396	18 017	17	–51 284	–41	–33 267	–31
Установка программного обеспечения	387 563	321 568	268 821	–65 995	–17	–52 747	–16	–118 742	–31
Управление приложениями	225 460	74 208	74 208	–151 252	–67	18 037	24	–133 215	–59
Конфигурация аппаратных средств	49 525	197 888	24 539	148 363	300	–173 349	–88	–24 985	–50
Установка аппаратных средств	120 721	123 680	41 130	2959	2	–82 550	–67	–79 591	–66
Управление дисками и файлами	29 736	74 208	14 963	44 472	150	–59 245	–80	–14 773	–50
Планирование вместимостью архива	8980	49 472	7252	40 492	451	–42 220	–85	–1729	–19
Резервное копирование и архивирование	130 654	123 680	50 622	–6974	–5	–73 058	–59	–80 032	–61
Управление архивами	0	24 736	0	24 736	Undefined	–24 736	–100	0	–
Общие ежегодные затраты	**1 563 387**	**2 473 600**	**836 474**	**910 213**	**58**	**–1 637 126**	**–66**	**–726 913**	**–46**

Табл. 12. ***Расшифровка затрат на обслуживание серверов***

Затраты на обслуживание серверов	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Решение проблем 2 уровня	73 882	85 592	29 237	11 711	16	–56 356	–66	–44 645	–60
Решение проблем 3 уровня	43 166	51 355	23 722	8189	19	–27 633	–54	–19 444	–45
Планирование и управление трафиком	18 721	21 398	9812	2677	14	–11 586	–54	–8908	–48
Точная настройка	18 721	12 839	9730	–5882	–31	–3109	–24	–8991	–48
Администрирование конечных пользователей	22 642	51 355	14 304	28 714	127	–37 051	–72	–8337	–37
Поддержка операционной системы	21 481	12 839	13 687	–8642	–40	848	7	–7794	–36
Обслуживание рабочей силы	17 026	21 398	10 481	4372	26	–10 917	–51	–6544	–38
Установка программного обеспечения	46 023	55 635	24 230	9612	21	–31 404	–56	–21 792	–47
Управление приложениями	28 751	12 839	12 434	–15 912	–55	–405	–3	–16 317	–57
Конфигурация аппаратных средств	143 021	34 237	94 451	–108 784	–76	60 215	176	–48 569	–34
Установка аппаратных средств	44 956	21 398	31 956	–23 558	–52	10 558	49	–13 000	–29
Управление дисками и файлами	27 732	12 839	16 619	–14 894	–54	3780	29	–11 114	–40
Планирование вместимостью архива	5783	8559	4175	2777	48	–4384	–51	–1607	–28
Резервное копирование и архивирование	24 229	21 398	20 786	–2831	–12	–612	–3	–3444	–14
Управление архивами	23 335	4280	20 423	–19 056	–82	16 143	377	–2913	–12
Общие ежегодные затраты	**559 468**	**427 961**	**336 049**	**–131 507**	**–24**	**–91 912**	**–21**	**–223 419**	**–40**

*Табл. 13. **Расшифровка затрат на планирование и управление процессами***

Затраты на планирование и управление процессами	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Управление стоимостью	69 097	0	67 866	–69 097	–100	67 866	Undefined	–1232	–2
Управление системными исследованиями планированием и продуктами	117 328	0	69 918	–117 328	–100	69 918	Undefined	–47 410	–40
Оценка закупок	86 071	0	76 853	–86 071	–100	76 853	Undefined	–9218	–11
Безопасность и защита от вирусов	169 951	0	103 863	–169 951	–100	103 863	Undefined	–66 088	–39
Затраты на восстановление бизнеса	18254	0	10 620	–18 254	–100	10 620	Undefined	–7634	–42
Общие ежегодные	**460 701**	**0**	**329 119**	**–460 701**	**–100**	**329 119**	**Undefined**	**–131 582**	**–29**

*Табл. 15. **Расшифровка финансовых и административных затрат***

Финансовые и административные затраты	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Затраты на контроль	388 410	199 511	317 198	–188 899	–49	117 688	59	–71 211	–18
Административная помощь сотрудникам ИТ-отдела	39 656	133 007	36 556	93 351	235	–96 451	–73	–3101	–8
Управление активами	70 323	66 504	17 374	–3819	–5	–49 129	–74	–52 949	–75
Бюджетирование	36 128	66 504	32001	30 375	84	–34 502	–52	–4127	–11
Аудит	18 032	33 252	10023	15 220	84	–23 229	–70	–8009	–44
Управление приобретением и контрактованием	84 239	133 007	54 290	48 768	58	–78 717	–59	–29 949	–36
Управление вендорами	159 048	33 252	107 883	–125 797	–79	74 632	224	–51 165	–32
Общие ежегодные	**795 837**	**665 036**	**575 326**	**–130 801**	**–16**	**–89 710**	**–13**	**–220 511**	**–28**

*Табл. 16. **Расшифровка затрат на поддержку конечных пользователей***

Затраты на поддержку конечных пользователей	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Затраты на поддержку	5 421 467	6 507 639	3 799 406	1 086 172	20	–2 708 233	–42	–1 622 061	–30
Затраты на самостоятельное изучение и поддержку	4 265 978	4 743 988	3 149 395	478 010	11	–1 594 593	–34	–1 116 583	–26
Формальное обучение	1 171 363	960 321	1 086 988	–211 041	–18	126 667	13	–84 375	–7
Управление данными	535 383	1 258 021	508 870	722 639	135	–749 151	–60	–26 512	–5
Разработка приложений	459 075	691 431	460 479	232 357	51	–230 953	–33	1404	0
Форс-мажор	0	6 296 965	0	6 296 965	Undefined	–6 296 965	–100	0	–
Общие ежегодные	**11 853 266**	**20 458 366**	**9 005 139**	**8 605 100**	**73**	**–11 453 227**	**–56**	**–2 848 127**	**–24**

С помощью программного продукта «TCO Manager» мы определили и получили текущий и целевой показатели совокупной стоимости владения. Теперь необходимо оценить доходную часть, объединяя метод ожидаемых потерь с таблицей оценки угроз и риска.

Методика Return on Investment for Security
(расчет возврата инвестиций в безопасность)

Первым шагом является построение таблицы TRA (таблица оценки угроз и рисков). Сделаем небольшое отступление и дадим краткое описание контрмер по обеспечению информационной безопасности. Контрмеры по обеспечению безопасности направлены на достижение следующих эффектов: уменьшение вероятности происхождения инцидента

и/или уменьшение последствий, если инцидент все равно случается. Меры, снижающие вероятность, называются профилактическими, а меры, снижающие по следствия, называются лечебными. Примеры контрмер обоих типов представлены в табл.17.

Табл.17. Типы контрмер безопасности

Тип контрмеры	Пример
Профилактические	1. Стандарты, процедуры, должностные инструкции 2. Аудит системы безопасности 3. Сетевые экраны 4. Системы обнаружения вторжений 5. Антивирусы 6. Средства шифрования 7. Формирование архивов
Лечебные	Резервные режимы работы
Принадлежат обоим типам	1. Планирование непрерывности бизнеса/ планирование восстановления бизнеса 2. Обучение

Пусть вероятность происшествия описана семью уровнями от «незначительного» до «экстремального». Определим эти уровни в табл.18.

Табл.18. Преобразование вероятности угроз к ежегодной частоте

Уровень вероятности	**Описание**	**Частота**
Незначительный	Вряд ли произойдет	0,05
Очень низкий	Событие происходит два-три раза в пять лет	0,6
Низкий	Событие происходит раз в год	1,0
Средний	Событие происходит раз в полгода	2,0
Высокий	Событие происходит раз в месяц	12,0
Очень высокий	Событие происходит несколько раз месяц	36,0
Экстремальный	Событие происходит несколько раз в день	365,0

Последствия от нарушения политики безопасности также описаны шестью уровнями от «несущественного» к «критическому», и каждому уровню соответствуют потери в случае ликвидации нарушений, которые определены экспертно специалистами Gartner Group (см. табл.19).

Табл.19. Последствия, преобразованные в стоимость ликвидации нарушений

Степень тяжести нарушения	**Описание**	**Потери, руб.**
Несущественная	При осознанной угрозе нарушение не будет иметь последствий	0
Низкая	Нарушение не ведет к финансовым потерям, но выявление хакера про- исшествия потребует значительных затрат	15 000
Существенная	Происшествие принесет некоторый материальный и моральный вред	150 000
Угрожающая	Потеря репутации, конфиденциальной информации. Затраты на восста-	1 500 000

	новление данных, проведение расследований	
Серьезная	Потеря клиентов, деловой репутации. Восстановление практически всех данных на электронных и бумажных носителях	3 000 000
Критическая	Потеря системы или перевод в другую безопасную среду	7 500 000

Теперь необходимо рассчитать показатель ALE (показатель ожидаемых потерь) для ЗАО «Страхование», используя форму таблицы (табл. 20), в которой сопоставляются вероятности угроз, степень тяжести нарушения и частота событий. Показатель ALE вычисляем согласно формуле:

$$ALE=f*L \quad (1)$$

где: *f* частота возникновения потенциальной угрозы, уровень которой определяется на основании вероятности (табл.18).

L величина потерь в рублях, которая определяется на основании степени тяжести нарушения (табл.19).

Табл. 20. Расчет показателя ожидаемых потерь для ЗАО «Страхование»

№	Актив	Потенциальная угроза	Вероятность	Последствия	Частота в год	Потери, руб.	ALE, руб.
1	Интернет-каналы	Разрушение ключевой инфраструктуры	Незначительный	Серьезная	0,005	3 000 000	150 000
		Отказ системы охлаждения	Средний	Существенная	2	150 000	300 000
		Нарушение конфиденциальности информации	Низкий	Серьезная	1	3 000 000	3 000 000
		Повреждение аппаратных средств инфраструктуры	Очень низкий	Угрожающая	0,6	1 500 000	900 000
		Неправильное построние инфраструктуры	Низкий	Существенная	1	150 000	150 000
		Атака на сетевую инфраструктуру провайдера	Очень низкий	Существенная	0,6	150 000	90 000
		Отказ DNS	Незначительный	Угрожающая	0,05	1 500 000	75 000
2	Система электронной почты	Атака на систему электронной почты	Очень высокий	Существенная	36	150 000	5 400 000
3	Бизнес-приложения	Проблема вывода документов на печать	Высокий	Несущественная	12	0	0
		Проблемы чтения/сохранения	Высокий	Несущественна	12	0	0

		файлов данных		я			
		Нарушения надежной работы бизнес-приложений	Низкий	Угрожающая	1	1 500 000	1 500 000
		Вывод из строя корпоративной системы документооборота	Высокий	Угрожающая	12	1 500 000	18 000 000
ИТОГО							**29 565 000**

Следующим шагом обоснования инвестиций в систему информационной безопасности является проведение анализа возврата инвестиций (табл.22). Первоначально определим затраты на внедрение системы информационной безопасности.

Для того чтобы обеспечить должный уровень безопасности, в ЗАО «Страхование» необходимо внедрить следующие элементы системы информационной безопасности: систему защиты интернет-шлюзов, систему антивирусной защиты файловых серверов и рабочих станций и систему защиты корпоративной электронной почты. Руководством в качестве поставщика решений была выбрана компания Trend Micro, которая представляет широкую линейку решений в области информационной безопасности для предприятий различного масштаба.

Затраты на внедрение комплекса решений Trend Micro приведены в табл.21.

Табл.21. Инвестиции в систему корпоративной защиты для ЗАО «Страхование»

№	Статьи затрат	Стоимость, руб.
1	Затраты на покупку лицензий	2 358 048
2	Затраты на проектные работы	369 785
3	Техническая поддержка (30% от стоимости лицензий ежегодно)	707 414

Период окупаемости инвестиционных проектов, связанных с внедрением информационных технологий, не должен превышать трех лет, поэтому период оценки эффективности данного проекта внедрения равен трем годам.

Табл. 22. Расчет показателей возврата инвестиций на систему информационной безопасности для ЗАО «Страхование»

Показатели	Начальные затраты, руб.	1 год, руб.	2 год, руб.	3 год, руб.	Общее, руб.
Затраты на внедрение	2 358 048	369 785	707 414	707 414	4 142 661
Накопленные затраты проекта внедрения	2 358 048	2 727 833	3 435 247	4 142 661	
Ставка дисконтирования	14 %				
Чистая приведенная стоимость (NPV) затрат на проект внедрения	3 645 614				
Текущий показатель ТСО	п/а	26 383 744	26 383 744	26 383 744	79 151 232

Целевой показатель ТСО	п/а	19 864 933	19 864 933	19 864 933	59 594 799
Фактический показатель ТСО	п/а	25 079 982	21 820 576	19 864 933	
Выгоды при оптимизации показателя ТСО	0	1 303 762	4 563 167	6 518 811	12 385 740
Показатель ожидаемых потерь (ALE)	0	29 565 000	29 565 000	29 565 000	88 965 000
Эффективность системы корпоративной защиты		85 %	85 %	85 %	
Ежегодные сбережения (AS)	0	50 268	3 309 674	5 265 317	
Показатель выгод при оптимизации показателя ТСО и ежегодныесбережения	0	1 354 030	7 872 841	11 784 128	21 010 999
Накопленный показатель выгод при оптимизации показателя ТСОи ежегодные сбережения	0	1 354 030	9 226 871	21 010 999	
Денежный поток	2 358 048	984 245	7 165 427	11 076 714	16 868 338
Накопленный денежный поток	2 358 048	1 373 803	5 791 624	16 868 338	
Чистая приведенная стоимость (NPV) доходов от проекта внедрения	10 577 426				
Внутренняя норма рентабельности (IRR)	145 %				

В первом случае роль денежного потока играют затраты на внедрение, а во втором это выгоды от оптимизации показателя ТСО и внедрения корпоративной системы защиты.

Ставка дисконтирования равна ставке рефинансирования Центрального Банка РФ. Внутренняя норма рентабельности рассчитывается при NPV равном нулю. Расчет точки безубыточности проекта внедрения корпоративной системы информационной безопасности выполнен графически (см. рисунок 1) и точка безубыточности равна 1,6 лет.

Таким образом, проект внедрения можно считать экономически выгодным, так как чистая приведенная стоимость доходов от проекта внедрения положительна и большечистой приведенной стоимости затрат на проект внедрения в 2,9 раза.

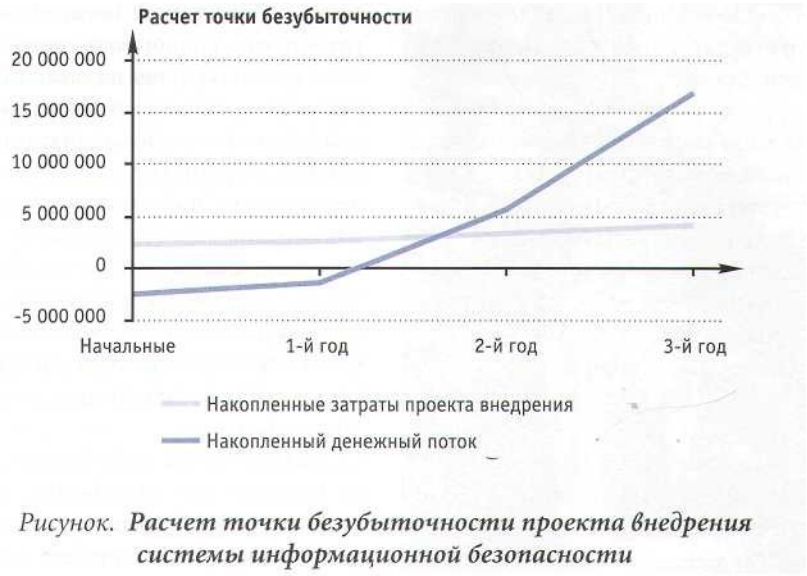

Рисунок. ***Расчет точки безубыточности проекта внедрения системы информационной безопасности***

Контрольные вопросы:

1. Какие методы оценки затрат на защиту информации вы знаете и дайте характеристику любого из них?
2. Какие затраты согласно методу «Совокупная стоимость владения» относятся к группе видимых?
3. Раскройте основные положения метода совокупной стоимости владения Total Cost of Ownership (TCO).
4. Составьте алгоритм расчета возврата инвестиций в безопасность согласно методике Total Cost of Ownership.

Практическая работа № 8. Отслеживание хода выполнения работ и фактических затрат по проекту в любой профессиональной сфере. Защита уровней обеспечения выполнения графика проекта

Цель работы

- Закрепить теоретические знания.
- Изучить основные экономические показатели и методы их расчета.
- Изучить технико-экономическое обоснование проектов с использованием новогооборудования.
- Изучить технико-экономическое обоснование проектирования автоматизированных информационных систем и программных продуктов.

Теоретическая часть.

Руководство любой компании понимает, что невозможно выделить неограниченный объем финансов и человеческих ресурсов на обеспечение информационной безопасности. С экономической точки зрения вложения в безопасность должны показать прибыль или сокращение имевших место или возможных затрат.

Невозможно создать абсолютно надежную систему безопасности. В основном изза того, что постоянно разрабатываются новые виды угроз, которым система не сможет противостоять, а также из-за того, что эффективность системы защиты зависит от обслуживающего персонала, а человеку свойственно ошибаться. Стоимость преодоления защиты должна быть больше стоимости достигаемого эффекта при ее взломе. В любом случае стоимость средств обеспечения безопасности должна соответствовать риску и прибыли для среды, окружающей хозяйствующий субъект.

Технико-экономическое обоснование проекта автоматизированной информационной системы проводится с целью:

- доказать целесообразность инвестиционного проекта по внедрению автоматизированной системы;
- рассчитать и проанализировать составляющие денежного потока для рассматриваемого срока службы системы;
- сопоставить затраты на создание и функционирование автоматизированной системы с результатами, получаемыми от ее внедрения, оценить прибыль, определить условия и сроки окупаемости затрат.

1. Показатели экономической эффективности проекта и методы их расчета

Показатели экономической эффективности проекта в целом характеризуют с экономической точки зрения технические, технологические и организационные решения, принимаемые в проекте. Эффективность ИП должна определяться на основе денежного потока, представляющего собой зависимость от времени денежных поступлений и платежей для всего расчетного периода.

При проведении экономических обоснований за расчетный период принимается временной интервал от начала действия проекта до его окончания. Расчетный период целесообразно разбить на шаги *(0, 1, …, m, …, n)*, используемые для оценки финансовых показателей. Разбивка обычно ведется для временного интервала год (квартал, месяц). Время в расчетном периоде измеряется в годах или долях года и отсчитывается от фиксированного момента времени $t0 = 0$, принимаемого за базовый. Обычно в качестве базового выбирается начало нулевого шага, а момент начала шага m обозначается t_m. При сравнивании нескольких проектов базовый момент рекомендуется выбирать одним и тем же.

Значение денежного потока обозначается $Ф(t)$, если оно относится к моменту времени t или $Ф(m)$, если оно относится к m–му шагу.

На каждом шаге значение денежного потока характеризуется: притоком, равным размеру денежных поступлений (результатов в стоимостном выражении) и оттоком, равным платежам на этом шаге. К притокам обычно относится выручка от реализации продукции, а также другие поступления. К оттокам – производственные издержки и налоги.

Термин «дисконтирование» широко употребляется в финансовой практике. Под ним можно понимать способ нахождения суммы *P* на некоторый момент времени *t* при условии, что в будущем при начислении на нее процентов, она могла бы составить наращенную сумму *S*. Величину *P*, найденную дисконтированием наращенной величины *S* называют приведенной величиной. С помощью дисконтирования в финансовых вычислениях учитывается фактор времени.

Для приведения разновременных затрат, результатов и эффектов используется норма дисконта *(E)*, равная норме дохода на капитал и выраженная в долях единицы или процентах в год.

Технически приведение денежного потока к базисному (обычно начальному) моменту времени осуществляется путем умножения его на коэффициент дисконтирования α_m, определяемой для постоянной нормы дисконта *E:*

$$\alpha_m = \frac{1}{(1+E)^m}, \quad (1.1)$$

где m – номер шага расчета ($m = 1, 2, \ldots, n$).

Если же норма дисконта меняется во времени и на шаге m равна E_m, то коэффициент дисконтирования определяется по формуле:

$$\alpha_0 = 1;$$

$$\alpha_m = \frac{1}{\prod_{k=1}^{m}(1+E_k)}; \text{при } t \quad (1.2)$$

$$k = 1$$

В рыночной экономике при использовании собственного капитала нормы дисконта определяются исходя из депозитного процента по вкладам, а на практике она выше этого процента за счет инфляции и риска, связанного с инвестициями. В случае, когда весь капитал заемный, норма дисконта представляет собой соответствующую процентную ставку, определяемую условиями процентных выплат и погашений по займам.

В мировой практике наибольшее распространение получил метод оценки экономической эффективности ИП с использованием следующих четырех показателей:

- чистого дисконтированного дохода;
- индекса доходности;
- внутренней нормы доходности;
- срока окупаемости капитальных вложений.

Наиболее общим и правильным является использование всех четырех взаимосвязанных показателей. При этом чистый дисконтированный доход – один из важнейших показателей и критериев эффективности, который в ряде случаев выступает как самостоятельная и единственная характеристика.

1.1. Чистый дисконтированный доход (ЧДД) характеризует превышение суммарных денежных поступлений над суммарными затратами для данного проекта с учетом неравномерности эффектов (затрат, результатов), относящихся к различным моментамвремени.

Основой для исчисления чистого дисконтированного дохода является «План денежных потоков», который строится путем анализа денежных притоков и оттоков. ЧДД рассчитывается по формуле:

$$ЧДД = \sum_{m=0}^{n} \alpha_m \quad (1.3)$$

Для признания проекта эффективным с точки зрения инвестора, необходимо, чтобы чистый дисконтированный доход (cash-flows) проекта был положительным. При проведении сравнительной оценки предпочтение следует отдать проекту с большим значением ЧДД (при выполнении условия его положительности). Очевидно, что при ЧДД > 0 проект следует принять, при ЧДД < 0 отвергнуть, а при ЧДД = 0 проект не прибылен, но и не убыточен.

Необходимо отметить, что ЧДД отражает прогнозную оценку изменения экономического потенциала предприятия в случае принятия рассматриваемого проекта. Этот показатель аддитивен во временном аспекте. Это очень важное свойство, выделяющее этот критерий из всех остальных и позволяющих использовать его в качестве основного при анализе оптимальности инвестиционного проекта.

Среди ученых нет единого мнения по вопросу методики определения ЧДД. Одни из них считают, что нужно ориентироваться на чистую прибыль (прибыль за вычетом налога на прибыль), получаемую при реализации проекта, другие считают, что необходимо учитывать при расчете амортизационные отчисления в виде притока денежных средств, т.е. не учитывать их в издержках.

где *К* – инвестиции, необходимые для реализации проекта; *П1 , П2 ,..., Пn* – чистая прибыль, получаемая по отдельным годам от реализации проекта; *Е* – норматив приведения затрат к единому моменту времени (норма дисконта).

Указанная позиция объясняется тем, что амортизационные отчисления – это средства, необходимые для осуществления процесса восстановления основных производственных фондов. Они остаются в распоряжении предприятия, т.е. это приток денежных средств, а не отток.

Часто ЧДД рекомендуется рассчитывается по следующей формуле:

где βm – индекс годового роста цен, показывает, во сколько раз в среднем увеличились цены за *m*-ый год.

В случае если к концу расчетного периода остается часть недоамортизированных основных фондов необходимо включить их остаточную стоимость в расчет ЧДД *в виде составляющего денежного потока на последнем шаге расчетного периода*. Остаточная стоимость основных фондов ориентировочно можно определить по формуле:

$$C_O = \sum_{x=1}^{y} C_x \left(1 - a_x t / 100\right), \qquad (1.7)$$

где $x...y$ – перечень имеющихся основных фондов (здания, оборудование и т.д.); Cx – первоначальная стоимость основных фондов х-го вида; a_x – норма амортизационных отчислений по х-м основным фондам, %; t – срок службы до завершения рассматриваемого расчетного периода, лет.

В настоящее время необходимо иметь ввиду, что существует развитая кредитная система, позволяющая осуществить капиталовложения, пользуясь банковским кредитом.

Наиболее часто встречающиеся кредиты – это кредит с погашением в рассрочку на протяжении T_K лет равными платежами (в номинальной стоимости). Тогда платежи с учетом процентов, которые включены в ежегодный платеж, по кредиту при заемной сумме Kn составят:

$$K_m = \frac{E_K \left(1 + E_K\right)^{T_K}}{\left(1 + E_K\right)^{T_K - 1}} \cdot K_n, \qquad (1.8)$$

где Km – платеж на m – том шаге с учетом процентов; E_K – номинальная годовая процентная ставка в банке.

1.2. Индекс доходности представляет отношение суммы приведенных эффектов к величине капитальных вложений. Показатель индекс доходности тесно связан с ЧДД. Он

строится из тех же элементов. Это означает, что как критериальный показатель из двух рассмотренных можно использовать один. В дальнейшем ограничимся использованием ЧДД.

1.3. Внутренняя норма доходности (норма рентабельности инвестиций). Под внутренней нормой доходности (ВНД) понимают значение ставки дисконтирования $E=E_{вн}$, при которой ЧДД проекта равен нулю. Схема расчета этого коэффициента при анализе ИП заключается в следующем: ВНД показывает максимально допустимый относительный уровень расходов, которые могут быть вложены в данный проект. Например, если проект финансируется за счет ссуды коммерческого банка, то значение ВНД показывает верхнюю границу допустимого уровня банковской процентной ставки, превышение которой делает проект убыточным.

На практике ИП может финансироваться из различных источников. В этом случае смысл показателя ВНД заключается в том, что разработчик должен сравнить полученное значение ВНД с ценой привлекаемых финансовых ресурсов (СС).

Если ВНД > СС, то проект следует принять, если ВНД < СС, то проект следует отвергнуть, если ВНД = СС – проект не прибыльный и не убыточный.

Чтобы определить ВНД нужно решить приводимое ниже уравнение относительно $E_{вн}$:

$$\sum_{0}^{m} \frac{Э_m - K}{(1 + E_{вн})^m} = 0, \qquad (1.9)$$

где K – дисконтированные капиталовложения (второе слагаемое уравнения 1.5); $Э_m$ – годовой доход ($П$).

$E_{вн}$ достаточно просто можно получить, если имеется одно поступление денежных средств и один платеж. Если же имеется ряд притоков и оттоков и они дисконтированы уравнение по поводу $E_{вн}$ не решается, а оценивается приближенно. Для этого используется специальный финансовый калькулятор. При его отсутствии может быть использован метод последовательных итераций с применением табулированных значений дисконтных множителей.

Расчет ведется с использованием уравнения:

$$ВНД = E_1 + \frac{ЧДД(E_1)}{ЧДД(E_1) - ЧДД(E_2)} \cdot (E_2 - E_1),$$

где $E1$ – значение процентной ставки в дисконтном множителе, минимизирующее положительное значение показателя ЧДД; $E2$ – значение процентной ставки в дисконтном множителе максимизирующее отрицательное значение ЧДД.

Сущность метода заключается в следующем:

Ориентируясь на существующие в момент анализа процентные ставки на ссудный капитал, выбирают два значения нормы дисконта $E1$ и $E2$ таким образом, чтобы в интервале $(E1, E2)$ функция ЧДД = $f(E)$ меняла свое значение с «+» на «-» или наоборот.

Далее используя формулу (1.10) производятся необходимые расчеты по определению $E_{вн}$. Точность вычислений обратна длине интервала (*E1* , *E2)*. Поэтому наименьшая аппроксимация достигается в случае, когда длина интервала составляет 1%.

1.4. Срок окупаемости. Сроком окупаемости называется время, за которое поступления от производственной деятельности предприятия покрывают затраты на инвестиции. Срок окупаемости измеряется в годах или месяцах.

Результаты и затраты, связанные с осуществлением проекта можно вычислять с дисконтированием и без него. Срок окупаемости с учетом дисконтирования называется периодом динамической амортизации и является наиболее точным. При расчетах срока окупаемости рекомендуется использовать дисконтирование как для притока, так и оттока денежных средств.

Алгоритм расчета срока окупаемости ($T_{ОК}$) зависит от равномерности распределения прогнозируемых доходов от инвестиций. Если доходы распределены по годам равномерно, то срок окупаемости рассчитывается делением единовременных затрат на величину годового дохода, обусловленного ими:

$$T_{Э} = \frac{K}{}, \quad — \qquad (1.11)$$

Если доход по годам распределяется неравномерно, то срок окупаемости рассчитывается прямым подсчетом числа лет, в течение которых инвестиции будут погашены кумулятивным доходом.

Практическая работа №9 Различные виды просмотра информации в проекте любой сферы, вывод отчётных данных проекта Специалисты в области управления проектами. Расчет капитальных вложений.

При проведении модернизации и внедрении нового оборудования в состав капитальных вложений предприятия включаются все единовременные затраты, которые должно нести предприятие в связи с переходом к эксплуатации более совершенных систем и оборудования.

Состав капитальных вложений в каждом конкретном случае различен и зависит от специфики проводимой модернизации. В общем случае капитальные вложения можно определить по формуле:

$$K_п = K_{пв} + K_с, \quad (2.1)$$

где $K_{пв}$ – прямые капитальные вложения, руб; $K_с$ – сопутствующие капитальные вложения, руб.

К прямым капитальным вложениям относятся совокупные затраты при приобретении оборудования. Сопутствующие капитальные вложения определяются суммой нескольких составляющих по выражению:

$$K_с = K_{дем} + K_{тр} + K_м + K_{зд} + K_{пр} + K_э + K_{иф}, \quad (2.2)$$

где $K_{дем}$ – единовременные затраты на демонтаж ранее установленного оборудова-

ния;

$K_{тр}$ – затраты на транспортировку нового оборудования к месту эксплуатации;

$K_м$ – затраты на установку, монтаж и наладку оборудования;

$K_{зд}$ затраты на строительство или реконструкцию здания, на необходимые произ-

водственные площади и другие элементы основных фондов, связанных с использованиемнового оборудования;

$K_{пр}$ – стоимость проекта;

$K_э$ – затраты на предотвращение отрицательных экологических последствий;

$K_{иф}$ – затраты на создание социальной инфраструктуры.

Основным методом определения сопутствующих капитальных вложений является метод прямого счета. Расчет отдельных составляющих капитальных вложений ведется на основе соответствующей проектно-сметной документации, действующих прейскурантов, ценников, норм и нормативов. Ориентировочно сопутствующие капиталовложения составляют 10…20% от стоимости нового оборудования.

Если капиталовложения вносятся не разово перед началом эксплуатации, их необходимо привести к расчетному году с учетом коэффициента дисконтирования. При использовании банковского кредита годовые платежи с учетом процентов также учитываются при формировании денежного потока (формула 1.8).

1.5. Расчет эксплуатационных расходов.

Основными составляющими годовых текущих издержек являются:

– заработная плата обслуживающего персонала;
– затраты на потребляемую электроэнергию;
– затраты на расходные материалы и запасные части;
– затраты на техническое обслуживание и текущие ремонты оборудования;
– ущерб, связанный с простоем оборудования при отказах.

Заработную плату обслуживающего персонала можно рассчитать по формуле:

100

где $Ч_О$ – численность обслуживающего персонала;

$t_О$ – время затрачиваемое на обслуживание устройства, мес.;

$S_З$ – среднемесячная заработная плата обслуживающего персонала, руб/мес;

k – коэффициент дополнительной заработной платы (1,1…1,2);

r – процент отчислений, на социальное страхование (35,6%).

Затраты на потребляемую электроэнергию учитывают мощность и время работы электроустановок, а также тариф на электроэнергию.

$$З_Э = \sum_{g=1}^{G} P_g t_g Ц_Э , \quad (2.4)$$

где $g \ldots G$ – перечень приемников электроэнергии;

P_g – потребляемая мощность токоприемников оборудования, кВт; t_g – действительный фонд времени работы оборудования, ч/год; $Ц_Э$ тариф на электроэнергию.

Затраты на вспомогательные материалы определяется по формуле:

$$S_М = m_М Ц_М , \quad (2.5)$$

где $m_М$ – норма расхода вспомогательного материала, кг/год;

$Ц_М$ – цена единицы вспомогательного материала, руб/кг.

Стоимость вспомогательных материалов можно принять в размере 5% от стоимости оборудования.

Определенные сложности представляет вычисление затрат на техническое обслуживание и ремонт оборудования. Указанная статья расходов вычисляется, если такая работа не входит в обязанности оперативного персонала и производится специальным подразделением.

Рассматриваемые затраты связаны с проведением плановых мероприятий и аварийными ремонтами.

$$S_р = S_{тор.} + S_a , \quad (2.6)$$

где $S_{тор}$ – стоимость плановых и технических обслуживаний и ремонтов согласно ежегодного графика профилактических мероприятий;

S_a – затраты, связанные с аварийно-восстановительными работами.

При этом стоимость плановых мероприятий можно определить по формуле:

$$S_{тор} = \sum_{i=1}^{n} S_{то.i} f_{то.i} C_{то.i.} + \sum_{i=1}^{n} S_{тр.i} f_{тр.i} C_{тр.i} , \quad (2.7)$$

где $S_{то.i}$, $S_{тр.i}$ – число технических обслуживаний и текущих ремонтов для i-го вида оборудования, шт;

$f_{то.i}$, $f_{тр.i}$ – трудоемкость проведения одного технического обслуживания и одного текущего ремонта i-го вида оборудования, чел.-ч;

$C_{то.i}$, $C_{тр.i}$ – стоимость проведения одного технического обслуживания и ремонта i-го вида оборудования, руб/чел.-ч.

Затраты на внеплановые ремонты можно определить, если располагать сведеньями об аварийности i-го вида оборудования, трудозатратами на их устранение и стоимостью работ.

$$S =$$

где P_i – процент ежегодного выхода из строя i-го вида оборудования от имеющегося, %;

N_i – число единиц оборудования i-го вида, шт;

$f_{ра.i}$ – трудоемкость устранения одного аварийного выхода из строя, чел.-ч;

$C_{ра.i}$ – стоимость одного чел.-ч работ для i-го вида оборудования.

Существует и более простой, но менее точный подход к определению затрат на ТОи ТР через нормативные показатели:

n

$S_p \bullet \sum Ци \bullet 1$ ——
$a_{pi^i} 100$
, (2.9)

где $i...n$ – перечень имеющегося оборудования;
$Ци$ – стоимость i-го вида оборудования, руб;
$apі$ – процент отчислений на ТО и ТР, %

Ущерб при отказах оборудования связан с недополучением прибыли из-за простоя оборудования или порчи продукции:

$$У \bullet \sum_{j \bullet 1}^{m} t_{пj} y_j \ , \qquad (2.10)$$

где $t_{пj}$ – суммарное время простоя по j-му технологическому процессу, ч;
yi – удельная величина технологического ущерба по j-му процессу, руб/ч.

Суммарные годовые текущие издержки:

$$И \bullet З_{.} З_{э.} S_{м.} S_{р.} У \ , \qquad (2.11)$$

1.6. Определение показателей экономической эффективности инвестиционногопроекта при внедрении новой техники.

Анализируемые в создаваемом проекте варианты технической реализации устройств и систем могут иметь различие в технико-экономических показателях. При этом отдельные технические характеристики опосредовано учитываются при расчете экономических показателей. Например, различная потребляемая мощность устройств учитывается при расчете потребляемой электроэнергии, повышение уровня электрификации и автоматизации процессов связано с изменением состава обслуживающего персонала, что может быть учтено при расчете заработной платы и т.д.

Для расчета показателей эффективности внедрения новых приборов нужно располагать такими характеристиками, как капитальные вложения и чистая прибыль. **Практическая часть.**

Вариант 1.

Задача 1. Для реализации проекта требуются инвестиции (капиталовложения), вносимые единовременно в размере 50 тыс. д.е. Чистые денежные притоки (чистая прибыль плюс амортизационные отчисления) по годам ориентировочно составят (тыс. д.е.) 1й год – 20; 2-й год – 22,5; 3-й год – 26; 4-й год – 32. Ставка дисконта составляет 20%. Сделать вывод об экономической целесообразности проекта на основе ЧДД.

Задача 2. Для задачи1 рассчитать ЧДД с учетом того, что в конце расчетного периода остаточная стоимость основных производственных фондов составит 10 тыс. д.е.

Задача 3. Требуется определить значение ВНД проекта системы информационной безопасности для ООО «Торговый дом ГАЗ», рассчитанного на 3 года, требующего инвестиций в размере 20 тыс. д.е. и имеющего предполагаемый приток денежных средств по годам: *П1 = 6 тыс. д.е.*, *П2 = 8 тыс. д.е.*, *П3 = 14 тыс. д.е.* Примечание: сравнить значение ВНД при Е1 = 15%, Е2 = 20% и Е1=16%, Е2=17%

Задача 4. На реконструкцию информационно-вычислительной сети «ЗАО Страхование» израсходовано 4,8 тыс. д.е. В результате доход за расчетный период по годам составил соответственно 1,2; 1,8; 2,0; 1,5; тыс. д.е. Ставка дисконта принята 20%. Требуется определить срок окупаемости проекта реконструкции с использованием дисконтированием и без него.

Вариант 2.

Задача 1. Для реализации проекта требуются инвестиции (капиталовложения), вносимые единовременно в размере 45 тыс. д.е. Чистые денежные притоки (чистая прибыль плюс амортизационные отчисления) по годам ориентировочно составят (тыс. д.е.) 1й год – 18; 2-й год – 22; 3-й год – 20; 4-й год – 25. Ставка дисконта составляет 15%. Сделать вывод об экономической целесообразности проекта на основе ЧДД.

Задача 2. Для задачи1 рассчитать ЧДД с учетом того, что в конце расчетного периода

остаточная стоимость основных производственных фондов составит 10 тыс. д.е.

Задача 3. Требуется определить значение ВНД проекта системы информационной безопасности для ООО «Торговый дом ГАЗ», рассчитанного на 3 года, требующего инвестиций в размере 18 тыс. д.е. и имеющего предполагаемый приток денежных средств по годам: *П1 =5 тыс. д.е.*, *П2 = 8 тыс. д.е.*, *П3 = 11 тыс. д.е.* Примечание: сравнить значение ВНД при Е1 = 15%, Е2 = 20% и Е1=16%, Е2=17%

Задача 4. На реконструкцию информационно-вычислительной сети «ЗАО Страхование» израсходовано 5 тыс. д.е. В результате доход за расчетный период по годам составил соответственно 1,1; 1,8; 2,2; 1,6 тыс. д.е. Ставка дисконта принята 18%. Требуется определить срок окупаемости проекта реконструкции с использованием дисконтированием и без него.

Вариант 3.

Задача 1. Для реализации проекта требуются инвестиции (капиталовложения), вносимые единовременно в размере 60 тыс. д.е. Чистые денежные притоки (чистая прибыль плюс амортизационные отчисления) по годам ориентировочно составят (тыс. д.е.) 1й год – 23; 2-й год – 22; 3-й год – 28; 4-й год – 45. Ставка дисконта составляет 18%. Сделать вывод об экономической целесообразности проекта на основе ЧДД.

Задача 2. Для задачи1 рассчитать ЧДД с учетом того, что в конце расчетного периода остаточная стоимость основных производственных фондов составит 10 тыс. д.е.

Задача 3. Требуется определить значение ВНД проекта системы информационной безопасности для ООО «Торговый дом ГАЗ», рассчитанного на 3 года, требующего инвестиций в размере 25 тыс. д.е. и имеющего предполагаемый приток денежных средств по годам: *П1 = 10 тыс. д.е.*, *П2 = 8 тыс. д.е.*, *П3 = 18 тыс. д.е.* Примечание: сравнить значение ВНД при Е1 = 15%, Е2 = 20% и Е1=16%, Е2=17%

Задача 4. На реконструкцию информационно-вычислительной сети «ЗАО Страхование» израсходовано 7 тыс. д.е. В результате доход за расчетный период по годам составил соответственно 2,2; 2,0; 3,1; 3,5 тыс. д.е. Ставка дисконта принята 16%. Требуется определить срок окупаемости проекта реконструкции с использованием дисконтированием и без него.

Вариант 4.

Задача 1. Для реализации проекта требуются инвестиции (капиталовложения), вносимые единовременно в размере 40 тыс. д.е. Чистые денежные притоки (чистая прибыль плюс амортизационные отчисления) по годам ориентировочно составят (тыс. д.е.) 1й год – 17; 2-й год – 21,5; 3-й год – 24; 4-й год – 25. Ставка дисконта составляет 11%. Сделать вывод об экономической целесообразности проекта на основе ЧДД.

Задача 2. Для задачи1 рассчитать ЧДД с учетом того, что в конце расчетного периода остаточная стоимость основных производственных фондов составит 10 тыс. д.е.

Задача 3. Требуется определить значение ВНД проекта системы информационной безопасности для ООО «Торговый дом ГАЗ», рассчитанного на 3 года, требующего инвестиций в размере 30 тыс. д.е. и имеющего предполагаемый приток денежных средств по годам: *П1 = 16 тыс. д.е.*, *П2 = 15 тыс. д.е.*, *П3 = 14 тыс. д.е.* Примечание: сравнить значение ВНД при Е1 = 15%, Е2 = 20% и Е1=16%, Е2=17%

Задача 4. На реконструкцию информационно-вычислительной сети «ЗАО Страхование» израсходовано 5,5 тыс. д.е. В результате доход за расчетный период по годам составил соответственно 0,9; 2,8; 3,0; 2,2 тыс. д.е. Ставка дисконта принята 13%. Требуется определить срок окупаемости проекта реконструкции с использованием дисконтированием и без него.

Вариант 5.

Задача 1. Для реализации проекта требуются инвестиции (капиталовложения), вносимые единовременно в размере 70 тыс. д.е. Чистые денежные притоки (чистая прибыль плюс амортизационные отчисления) по годам ориентировочно составят (тыс. д.е.) 1й год – 28; 2-й год – 32; 3-й год – 30; 4-й год – 35. Ставка дисконта составляет 25%. Сделать вывод об экономической целесообразности проекта на основе ЧДД.

Задача 2. Для задачи1 рассчитать ЧДД с учетом того, что в конце расчетного периода остаточная стоимость основных производственных фондов составит 10 тыс. д.е.

Задача 3. Требуется определить значение ВНД проекта системы информационной

безопасности для ООО «Торговый дом ГАЗ», рассчитанного на 3 года, требующего инвестиций в размере 22 тыс. д.е. и имеющего предполагаемый приток денежных средств по годам: *П1 = 8 тыс. д.е.*, *П2 = 11 тыс. д.е.*, *П3 = 13 тыс. д.е.* Примечание: сравнить значение ВНД при Е1 = 15%, Е2 = 20% и Е1=16%, Е2=17%

Задача 4. На реконструкцию информационно-вычислительной сети «ЗАО Страхование» израсходовано 6,3 тыс. д.е. В результате доход за расчетный период по годам составил соответственно 1,5; 1,9; 2,7; 1,9 тыс. д.е. Ставка дисконта принята 18%. Требуется определить срок окупаемости проекта реконструкции с использованием дисконтированием и без него.