ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №1
ОЦЕНКА НЕОБХОДИМОСТИ ЗАЩИТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ

1 Краткие теоретические сведения

Информация может проявляться в различных формах, воздействующих на органы чувств и поведение человека. Руководителя организации из всех возможных форм существования информации должны интересовать в первую очередь такие, которые несут смысловую нагрузку. К ним могут быть отнесены речевая, документальная (рукописная, печатная, текстовая, цифровая, графическая), видовая (фото, телевизионная) и т.п. Каждая из этих форм может включать как общедоступные сведения, так и сведения, содержание которых предназначено для ограниченного круга лиц. Из всех форм наиболее доступной, распространенной и насыщенной содержанием является **речевая информация**. Через речевую форму информации практически проходит каждая из любых других форм. Представляется, что речевая информация, преобладая по объему над всеми остальными, несет наибольшую часть конфиденциальных сведений. В силу массовости, этот вид информации является трудно контролируемым по содержанию и трудно защищаемым в части конфиденциальности. Поэтому данному виду информации должно быть уделено максимальное внимание.

Высокая стоимость конфиденциальных сведений о деятельности конкурирующих структур показывает, что проблема защиты информации (ЗИ) от перехвата ее техническими средствами и агентами конкурентов весьма актуальна как для государственного, так и негосударственного сектора. Особенно острым является вопрос о необходимости защиты конфиденциальной информации негосударственного сектора. Это обусловлено тем, что государственный сектор серьезно занимается ЗИ и имеет солидный научно-технический потенциал, силы и технические средства для решения этих задач; негосударственный же сектор в вопросах ЗИ в стране делает первые шаги в отличие от государственного и частных фирм зарубежных стран, где этому вопросу уделяется большое внимание. Отсутствие подготовленных специалистов, научных проработок, опыта, знаний, необходимых документов и технических возможностей фирм у этого сектора в условиях конкуренции ставит их в затруднительное, неравное с предприятиями госсектора положение.

Задача создания простых методических материалов, позволяющих руководителям грамотно организовать ЗИ на своих предприятиях, весьма актуальна.

Решение о необходимости защиты принимается на основе оценок по двум направлениям:

1. Наличие конфиденциальной информации и опасность ее утечки;
2. Экономическая необходимость (целесообразность) защиты конфиденциальной информации.

Методика предназначена для проведения общей и частных оценок, позволяющих руководителю организации принять обоснованное решение о необходимости защиты конфиденциальной информации, циркулирующей внутри организации, от конкурентов с оценкой предстоящих расходов на защиту. Методика позволяет быстро и достаточно объективно провести экспресс-оценку необходимости защиты конфиденциальной информации и на ее основе оперативно принять соответствующее решение, т.е. она позволяет руководителю избежать больших коммерческих неудач и потерь прибыли из-за доступности информации конкурентам без

длительного пути самоубеждения на собственных ошибках и потерях о необходимости защиты конфиденциальной информации.

Решение о необходимости защиты конфиденциальной информации, циркулирующей внутри организации, должно приниматься руководством организации и в первую очередь ее учредителем. Никто не заинтересован в такой мере в защите секретов организации, и никто так не знает всю совокупность циркулирующей на фирме информации, ее степень секретности, внутреннюю и внешнюю обстановку, как ее учредитель.

Методика состоит из двух взаимосвязанных частей. Первая часть позволяет на основе обработки результатов анкетного опроса принципиально ответить на вопрос, нужно или не нужно защищать информацию, циркулирующую на фирме, а вторая часть, в случае положительного решения первого вопроса, позволяет приближенно оценить затраты на предстоящую ЗИ.

Учитывая заинтересованность, компетентность и кругозор учредителя организации, предложена методика, которая максимально учитывает знания, опыт и мнение самого учредителя организации. В основу первой части методики положен метод анкетного опроса с последующей обработкой его результатов.

Для реализации данного метода разработан перечень анкетных вопросов для учредителя организации, охватывающий основные стороны деятельности организации, связанные с циркулирующей в ней информацией.

Перечень анкетных вопросов

Вопросы анкеты сформулированы таким образом, что не требуют пространных ответов, а сводятся к односложным ответам «да», «нет». Заполнение анкеты не требует специальной подготовки в области ЗИ и не вызывает трудностей и больших временных затрат. Специальные знания по ЗИ учтены при разработке анкетных вопросов и при последующей обработке результатов опроса с участием специалистов по ЗИ.

Количественная оценка наличия конфиденциальной информации в организации и необходимости ее защиты получается путем математической обработки ответов на анкетные вопросы. С этой целью каждому вопросу анкеты поставлена в соответствие весовая величина, численно выражающая долевой вклад содержания вопроса в необходимость защиты конфиденциальной информации. Значения весовых коэффициентов получены экспертным методом.

При обработке результатов анкетного опроса можно получить как общую оценку необходимости защиты на фирме, так и ряд частных оценок по возможным направлениям защиты. Совокупность всех оценок позволяет руководителю, в конечном счете, принять решение о необходимости организации защиты путем проведения режимных, организационных и технических мер.

На основе анализа полученных оценок выявляются те звенья защиты, где она не обеспечена и вероятность перехвата информации конкурентом (утечка) недопустимо высока. Проведя такой анализ, руководитель организации может целенаправленно проводить работы по устранению утечки информации по выявленным направлениям.

Порядок проведения оценок и существо первой части методики заключается в следующем.

На первом этапе заинтересованная в ЗИ сторона в лице учредителя или руководителя организации заполняет анкету, отвечая на ее вопросы, приведенные в таблице 1. Ответы на вопросы анкеты в форме «да» или «нет» заносятся в графу 3 против соответствующих вопросов (см. таблица 2).

На втором этапе с привлечением консультанта проводится анализ результатов опроса. **Если ответ на вопрос соответствует увеличению опасности утечки информации, то в графе 4 таблицы 2 проставляется знак «+», в противном случае проставляется знак «-».**

Таблица 1 – Перечень вопросов анкеты

№ п/п	Вопросы анкеты	Долевые коэффициенты для общей оценки	Долевые коэффициенты для частных оценок
1	2	3	4
Уровень конкуренции			
1	1) Конкурентоспособна ли Ваша продукция на внутреннем рынке?	3,5	35
	2) Конкурентоспособна ли Ваша продукция на внешнем рынке?	5,0	50
	3) Монопольна ли Ваша продукция на внутреннем рынке?	1,5	15
Степень конфиденциальности информации, циркулирующей на фирме			
2	1) Имеется ли информация, предназначенная только лицам верхнего звена управления, с грифом «строго конфиденциально»?	11,0	55
	2) Имеется ли информация, предназначенная ограниченному кругу лиц, выполняющих конкретные операции и задания, в части их касающаяся, с грифом «конфиденциально»?	5,0	25
	3) Имеется ли информация ограниченной доступности только работникам организации?	4,0	20
Время «старения» конфиденциальности информации			
3	1) Носит ли конфиденциальность долговременный характер (год и более)?	5,0	50
	2) Носит ли конфиденциальность кратковременный характер (месяц и более)?	4,0	40
	3) Носит ли конфиденциальность оперативный характер (до месяца)?	1,0	10
Режимные и организационные мероприятия			
4	1) Учитываются ли интересы сохранения тайны организации при кадровом отборе верхнего звена управления?	3,8	13
	2) То же при подборе лиц, которые будут допущены к конфиденциальной информации?	2,7	9
	3) То же при кадровом отборе штатного персонала организации в целом?	1,5	5
	4) Налажен ли контроль за сохранением работниками организации коммерческой тайны?	1,8	6

Продолжение таблицы 1

1	2	3	4
	5) Обеспечена ли охрана организации и защита конфиденциальной документации, содержащей коммерческую тайну?	2,2	7,4
	6) Возможен ли доступ «недопущенных» лиц к средствам размножения и обработки информации, отнесенной к указанным в пункте 2 категориям конфиденциальности?	2,3	7,6
	7) Возможно ли, по Вашему мнению, проникновение агента конкурирующей организации в верхнее звено управления?	6,0	19,7
	8) То же в среднее звено управления?	3,7	12,3
	9) То же в обслуживающий технику персонал?	2,3	7,6
	10) То же в персонал, выполняющий работы, прямо не связанные с конфиденциальной информацией?	1,5	5
	11) Выделено ли специальное помещение для совещаний и переговоров с деловыми партнерами?	2,5	7,4
Оснащение служебных помещений техническими средствами			
5	1) Проводными телефонами?	2,5	10,5
	2) Переговорными устройствами (рациями)?	1,5	5
	3) Датчиками пожарной и охранной сигнализации?	0,6	2
	4) Электронными часами?	0,8	2,5
	5) Абонентскими громкоговорителями?	0,9	3
	6) VoIP-телефонами?	1,5	7
	7) Установками прямой телефонной связи?	1,3	7
	8) Радиоприемниками?	1,5	5
	9) Телевизорами?	1,5	5
	10) DVD-проигрывателями?	0,5	1,5
	11) Диктофонами?	0,5	1,5
	12) Радиотелефонами?	1,5	7
	13) Установкой оперативной (директорской) телефонной связи?	1,5	7
	14) Телефаксами?	2,2	7,5
	15) Персональными компьютерами?	6,0	13,5
	16) Системами видеонаблюдения?	0,9	3
	17) Автоматической телефонной станцией?	4,5	12

На третьем этапе производится суммирование долевых коэффициентов графы 5, соответствующих знаку «+» по всем вопросам анкеты. Результат суммирования является общей оценкой (G) для принятия решения о необходимости защиты конфиденциальной информации организации в целом.

Таблица 2 – Результаты анализа ответов на вопросы анкеты (пример)

Анкеты	№ вопроса по пунктам анкеты	Ответы на вопросы анкетируемого	Результаты анализа ответов	Долевые коэффициенты для общей оценки	Долевые коэффициенты для частных оценок	Общая оценка	Частные оценки
1	2	3	4	5	6	7	8
1	1	да	+	3,5	35	56,5	35
	2	нет	-	5,0	50		
	3	нет	-	1,5	15		
2	1	да	+	11	55		100
	2	да	+	5,0	25		
	3	да	+	4,0	20		
3	1	да	+	5,0	50		90
	2	да	+	4,0	40		
	3	нет	-	1,0	10		
4	1	да	-	3,8	13		50,9
	2	да	-	2,7	9		
	3	нет	+	1,5	5		
	4	нет	+	1,8	6		
	5	да	-	2,2	7,4		
	6	да	+	2,3	7,6		
	7	нет	-	6,0	19,7		
	8	да	+	3,7	12,3		
	9	да	+	2,3	7,6		
	10	да	+	1,5	5		
	11	нет	+	2,5	7,4		
5	1	да	+	2,5	10,5		32
	2	да	+	1,5	5		
	3	да	-	0,6	2		
	4	да	+	0,8	2,5		
	5	нет	-	0,9	3		
	6	да	+	1,5	7		
	7	нет	-	1,3	7		
	8	да	+	1,5	5		
	…	…	…	…	…		

Если общая оценка меньше 20 ($G < 20$), то **вероятность утечки информации мала и защиту информации можно не проводить.** Если общая оценка G больше 20, но меньше 50 ($20 \le G < 50$), то вероятность утечки информации достаточно велика, **необходимо рассмотреть частные оценки**, возможно защита необходима по отдельным направлениям. Если общая оценка G равна или больше 50 ($G \ge 50$), то **защиту необходимо проводить по всем направлениям.**

На четвертом этапе проводится анализ с помощью частных оценок по всем 5 группам опросной анкеты. Для получения частных оценок проводят суммирование долевых коэффициентов графы 6 таблицы 2, помеченных знаком «+» для каждой группы отдельно. При этом получится пять частных оценок:

1) по пункту 1 – оценка конкурентоспособности продукции (услуг) – G1;

2) по пункту 2 – оценка степени конфиденциальности информации – G2;

3) по пункту 3 – оценка временных характеристик конфиденциальности информации – G3;

4) по пункту 4 – оценка необходимости ЗИ режимными и организационными методами – G4;

5) по пункту 5 – оценка возможности утечки информации через технические средства – G5.

Если частная оценка по каждому из пунктов 1-3 равна или больше 20 (G 1, 2, 3 ≥ 20), то **это подтверждает необходимость ЗИ в организации.** Если частная оценка по 4 и 5 пунктам равна или больше 20 (G 4, 5 ≥ 20), то **это указывает на необходимость проведения ЗИ режимными и организационными методами или с помощью технических средств защиты соответственно.** В том случае, если частная оценка меньше 20 (G 1, 2, 3, 4, 5 < 20), то **ЗИ по данной группе вопросов можно не проводить.**

Таким образом, если на основе полученных оценок руководитель организации принимает решение о необходимости проведения работ по организации ЗИ, то вполне естественно, что перед руководителем организации встает другой очень важный вопрос о предстоящих затратах на организацию ЗИ. Этот вопрос решается с помощью второй части методики.

Вторая часть методики предназначается для проведения ориентировочной оценки ожидаемых затрат, связанных с защитой речевой и других видов информации, используемых в деятельности организации, например, информации в печатном виде и обрабатываемой на ПК.

В общем случае затраты на ЗИ складываются из затрат на проведение организационно-режимных и технических мер. Затраты на режимные и организационные меры ЗИ определяются главным образом заработной платой работников режимных подразделений, обеспечивающих организацию и контроль режимных мер, повышающих безопасность конфиденциальной информации. В свою очередь, затраты на техническую защиту складываются из затрат на проведение исследований, позволяющих выявить каналы утечки информации и определить способы их устранения, и из ожидаемых затрат на реализацию технических решений защиты информации.

Расчет стоимости защитных мероприятий каждого из видов информации имеет некоторые особенности, но на этапе ориентировочных расчетов можно использовать методику защиты речевой информации как наиболее простой и общей. Такая методика, являющаяся второй составной частью общей методики оценки, представлена ниже. Учитывая, что методика предназначена для проведения экспресс-оценки стоимости ЗИ, позволяющей руководителю организации приблизительно оценить предстоящие затраты, она максимально упрощена и предусматривает проведение элементарных расчетов. С этой целью все техническое оборудование, которое может быть установлено в организации и через которое возможна утечка информации (в соответствии с 5 пунктом анкетных вопросов), условно разделено на три группы. Критерием такого деления выбрана степень защищенности оборудования, предусмотренная ее производителем, т.е. для более простых устройств долевой коэффициент затрат будет выше, чем для более сложных, предполагающих наличие самостоятельных механизмов защиты. Перечень технического оборудования по группам с указанием формул для расчета величины затрат на защитные мероприятия приведен в таблице 3.

Таблица 3 – Стоимость защиты оборудования

Группа	Перечень оборудования	Величина затрат на защиту оборудования от утечки информации	Величина затрат на ежегодный профилактический контроль эффективности ЗИ
1	2	3	4
1	Проводные телефоны; переговорные устройства (рации); датчики пожарной и охранной сигнализации; электронные часы; абонентские громкоговорители	$K_1 = 0{,}7 \cdot C_1$	$K_{проф} = (0{,}05 \ldots 0{,}1) \cdot (C_1 + C_2 + C_3)$
2	VoIP-телефоны; установки прямой телефонной связи; радиоприемники; телевизоры; диктофоны; DVD-проигрыватели; радиотелефоны	$K_2 = 0{,}3 \cdot C_2$	
3	Пульты оперативной (директорской) телефонной связи до 100 номеров; телефаксы; персональные компьютеры; системы видеонаблюдения; АТС на 100-1000 номеров	$K_3 = 0{,}15 \cdot C_3$	

В таблице обозначено: C_1, C_2, C_3 – суммарная стоимость технического оборудования соответствующей группы, установленного в организации. Значения стоимости образцов техники, находящихся в помещениях организации, определяются по каталогам действующих цен изготовителя данной техники (можно воспользоваться приближенными ценами из таблицы 4).

Стоимость технической защиты всего оборудования ($C_{тз}$), состоящего из техники различных групп, определяется по формуле:

$$C_{тз} = K_1 + K_2 + K_3 \qquad (1)$$

Примечание: в таблице 3 не приводится расчет стоимости защиты специального оборудования, используемого для передачи, обработки и хранения конфиденциальной информации. Стоимость защиты такого оборудования определяется индивидуально и может существенно превышать указанную в таблице 3.

Стоимость ежегодного профилактического контроля определяется по формуле:

$$C_{проф} = K_{проф} \qquad (2)$$

Таким образом, зная перечень и количество установленного в организации технического оборудования и его стоимость, можно без труда рассчитать общие ожидаемые затраты на ЗИ техническими средствами:

$$C_{общ.з.} = C_{тз} + C_{роз} + C_{проф} \qquad (3)$$

где $C_{роз}$ – ежегодные затраты на режимные и организационные меры, которые определяются заработной платой работников службы информационной безопасности. В случае отсутствия данной службы коэффициентом можно пренебречь.

Получив такие оценки, руководитель организации принимает решение на проведение работ по защите информации.

Таблица 4 – Приблизительная стоимость технических средств

Наименование	Стоимость, дол. США
1	2
1) Проводные телефоны	30
2) Переговорные устройства (рации)	35
3) Датчики пожарной / охранной сигнализации	10 / 25
4) Электронные часы	20
5) Абонентские громкоговорители	30
6) VoIP-телефоны	70
7) Установки прямой телефонной связи	15
8) Радиоприемники	20
9) Телевизоры	250
10) DVD-проигрыватели	50
11) Диктофоны	40
12) Радиотелефоны	45
13) Установки оперативной (директорской) телефонной связи	500
14) Телефаксы	150
15) Персональные компьютеры	700
16) Системы видеонаблюдения	300
17) Автоматические телефонные станции	3000

2 Практическое задание

1. Составить описание организации, род деятельности которой – сфера информационных технологий или любая другая область, но в основе которой лежит информационная система. Указать, какая конфиденциальная информация находится в организации. Ответить на вопросы анкеты из таблицы 1, оформив результаты по примеру таблицы 2.

2. Провести оценку необходимости защиты конфиденциальной информации в данной организации в соответствии с приведенной методикой. Сделать вывод о необходимости защиты информации в организации.

3. Оценить ожидаемые затраты на обеспечение безопасности информационной системы. Сделать вывод о готовности организации затратить полученную сумму на защитные мероприятия.