Практическая работа №3

ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цель работы. Изучить методики оценки рисков и необходимости защиты информационной системы. Научиться рассчитывать риски, используя количественную и качественную методики.

Краткие сведения из теории

Управление информационными рисками – системный процесс идентификации, контроля и уменьшения информационных рисков компаний в соответствии с определенными ограничениями нормативно-правовой базы (НПБ) в области защиты информации и собственной корпоративной политики безопасности.

Защита активов связана с деятельностью по предотвращению угроз, классифицируемых в зависимости от характера ущерба, который они могут нанести этим активам. Во внимание должны приниматься все угрозы, но в первую очередь те, которые связаны со случайными и преднамеренными действиями человека.

Основной нормативно-правовой базой являются международные стандарты ISO 17799 и ISO 13335. Согласно СТБ 34.101.1–2014 риск нарушения безопасности – это возможность реализации угрозы, которая нанесет ущерб владельцу. Так же под риском понимают сочетание вероятности события и его последствий.

Суть количественной оценки рисков сводится к поиску единственного оптимального решения из множества существующих. Например, необходимо ответить на следующие вопросы: «Как, оставаясь в рамках утвержденного годового (квартального) бюджета на информационную безопасность, достигнуть максимального уровня защищенности информационных активов компании?» или «Какую из альтернатив построения корпоративной защиты информации (защищенного *WWW* сайта или корпоративной *E-mail*) выбрать с учетом известных ограничений бизнес-ресурсов компании?» К количественным методикам управления рисками относятся методики *CRAMM*, *MethodWare* и др. Рассмотрим наиболее распространённую из них.

CRAMM. Управление рисками в методике *CRAMM* осуществляется в несколько этапов. На первом этапе инициализации – «*Initialization*» – определяются границы исследуемой информационной системы компании, состав и структура ее основных физических и информационных активов и транзакций. Первичная информация собирается в процессе бесед с менеджерами проектов, менеджером пользователей или другими сотрудниками.

На втором этапе идентификации и оценки ресурсов – «*Identification and Valuation of Assets*» – четко идентифицируются активы и определяется их стоимость. Расчет стоимости информационных активов однозначно позволяет определить необходимость и достаточность предлагаемых средств контроля и защиты.

На третьем этапе оценивания угроз и уязвимостей – «*Threat and Vulnerability Assessment*» – идентифицируются и оцениваются угрозы и уязвимости информационных активов компании. Для такой оценки и идентификации в коммерческом варианте метода *CRAMM* (профиль *Standard*, в других вариантах совокупность будет иной, например, в версии, используемой в правительственных учреждениях, добавляются параметры, отражающие такие области, как национальная безопасность и международные отношения) используется следующая совокупность критериев (последствий реализации угроз информационной безопасности): критерий 1 – ущерб репутации организации; 2 – финансовые потери, связанные с восстановлением ресурсов; 3 – дезорганизация деятельности компании; 4 – финансовые потери от разглашения и передачи информации конкурентам, а также другие критерии.

Четвертый этап анализа рисков – «*Risk Analysis*» – позволяет получить количественные оценки рисков. Эти оценки могут быть рассчитаны по формулам (1) – (4):

$$R = P_{\text{ущ}} C_{\text{ущ}}; \tag{1}$$

$$R = P_{\text{угр}} P_{\text{уяз}} C_{\text{ущ}}, \tag{2}$$

где R – величина риска в результате реализации угрозы;

$P_{\text{ущ}}$ – вероятность ущерба в результате реализации угрозы;

$P_{\text{угр}}$ – вероятность реализации угрозы;

$P_{\text{уяз}}$ – вероятность реализации уязвимости;

$C_{\text{ущ}}$ – величина ущерба в результате реализации угрозы.

Если информационный объект (ИО) подвержен нескольким (N) угрозам (критериям оценки возможного ущерба), то совокупный риск ($R_{\text{общ}}$) нанесения злоумышленниками ущерба ИО может быть представлен как

$$R_{\text{общ}} = \sum_{i=1}^{N} P_i \cdot C_i, \tag{3}$$

где C_i – цена ущерба по i-й угрозе;

P_i – вероятность ущерба i-й угрозы, выбираемый экспертами из условия

$$\sum_{i=1}^{N} P_i = 1 \cdot \tag{4}$$

На пятом этапе управления рисками – «*Risk management*» – предлага-

ются меры и средства уменьшения или уклонения от риска. Возможно проведение коррекции результатов или использование других методов оценки. Полученные уровни угроз, уязвимостей и рисков анализируются и согласовываются с заказчиком. Только после этого можно переходить к заключительной стадии метода.

На заключительной стадии *CRAMM* генерирует несколько вариантов мер противодействия, адекватных выявленным рискам и их уровням. Контрмеры разбиваются на группы и подгруппы по следующим категориям:

− обеспечение безопасности на сетевом уровне;

− обеспечение физической безопасности;

− обеспечение безопасности поддерживающей инфраструктуры;

− меры безопасности на уровне системного администратора.

Защита активов связана с деятельностью по предотвращению угроз, классифицируемых в зависимости от характера ущерба, который они могут нанести этим активам. Во внимание должны приниматься все угрозы, но в первую очередь те, которые связаны со случайными и преднамеренными действиями человека. На рисунке 1 приведены концептуальные понятия безопасности и их взаимосвязь, регламентируемые СТБ 34.101.1–2014.

В защите активов заинтересованы их собственники (владельцы). Но эти активы представляют интерес и для нарушителей, которые стремятся использовать активы в своих целях, вопреки интересам владельцев. Нарушения безопасности обычно включают (но не ограничиваются только этими категориями): несанкционированное раскрытие (потерю конфиденциальности), несанкционированную модификацию (потерю целостности) или несанкционированное лишение доступа к активам (потерю доступности).

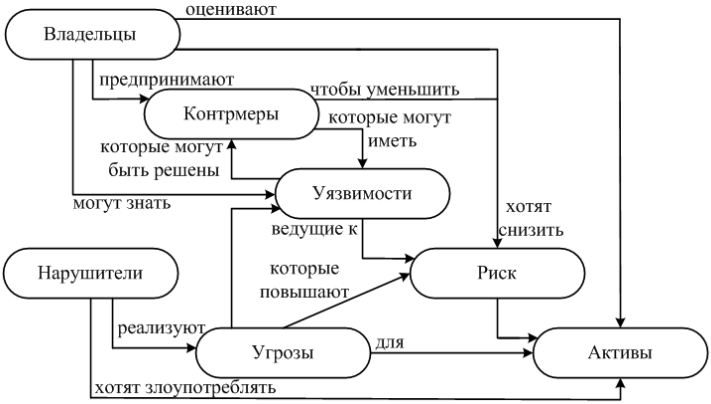

Рисунок 1 – Схема концептуальных понятий безопасности и их взаимосвязь

Владельцы активов должны проводить анализ риска, т. е. определять угрозы, уязвимые места, возможный ущерб от реализации каждой угрозы и контрмеры. Чтобы выполнялась требуемая владельцем политика безопасности активов, необходимо принять меры по уменьшению числа уязвимых мест, так как нарушители могут их использовать.

Еще до ввода в эксплуатацию системы (продукта) ИТ владелец заинтересован в оценке эффективности мер противодействия угрозам. Результатом такой оценки является заключение о степени гарантии, с которой меры противодействия уменьшают риск для активов. Гарантией называется основание для уверенности в том, что система (продукт) ИТ отвечает задачам безопасности.

Качественная 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.

Решение о необходимости защиты конфиденциальной информации, циркулирующей внутри организации, должно приниматься руководством организации. Никто не заинтересован в такой мере, как руководство, в защите секретов организации, и никто так не знает всю совокупность циркулирующей в организации 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 в организации, а вторая часть, в случае положительного решения первого вопроса, позволяет приближенно оценить затраты на предстоящую защиту информации (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 все стороны деятельности организации, связанные с циркулирующей на ней информацией.

Вопросы анкеты сформулированы таким образом, что не требуют пространных ответов, а сводятся к односложным ответам «да», «нет». Заполне-

ние 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 о состоянии и необходимости дополнительной 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 общую систему защиты конфиденциальной информации. Значения весовых коэффициентов получены экспертным методом.

При обработке результатов анкетного опроса можно получить как общую оценку состояния защиты в организации, так и ряд частных оценок по 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 оценок каждой составляющей защиты выявляются те ее звенья, где ЗИ не обеспечена и вероятность ее перехвата 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 руководителя организации заполняет анкету, отвечая на ее вопросы, приведенные в приложении А. Ответы на вопросы анкеты в форме «да» или «нет» заносятся в столбец 3 таблицы 1 против соответствующих вопросов.

На втором этапе с привлечением консультанта проводится анализ результатов опроса. Если ответ на вопрос соответствует увеличению опасности утечки информации, то в столбце 4 таблицы 1 проставляется знак «+», в противном случае проставляется знак «–».

На третьем этапе производится суммирование долевых коэффициентов столбца 5, соответствующих знаку «+» по всем вопросам анкеты. Долевые коэффициенты для каждого вопроса представлены в приложении Б. Результат суммирования является общей оценкой (G) для принятия решения о необходимости защиты конфиденциальной информации в организации в целом. При этом если общая оценка G равна или больше 50 ($G > 50$), то **защиту необходимо проводить по всем направлениям.**

Если общая оценка G больше 20, но меньше 50 ($50 > G > 20$), то вероятность утечки информации достаточно велика, необходимо провести частные оценки, защита необходима по отдельным направлениям. Если общая оценка меньше 20 ($G < 20$), то **вероятность утечки информации мала и до-**

полнительную защиту информации можно не проводить.

На четвертом этапе проводится анализ с помощью частных оценок по всем пяти пунктам опросной анкеты. Для получения частных оценок проводят суммирование долевых коэффициентов столбца 6 таблицы 1, помеченных знаком «+» для каждого пункта отдельно. При этом получится пять частных оценок (таблица 2).

Таблица 1 – **Расчет частных и общих оценок рисков по качественной методике**

Анкеты	№ вопроса по пунктам анкеты	Ответы на вопросы анкетируемого	Результаты анализа ответов	Долевые коэффициенты оценок		Оценки	
				общей	частных	общая	частные
1	2	3	4	5	6	7	8
1	1						
	2						
	3						
2	1						
	2						
	3						
3	1						
	2						
	3						
4	1						
	2						
	…						
	11						
5	1						
	2						
	…						
	18						

Таблица 2 – **Частные оценки**

Анкеты	Частная оценка
1	Конкурентоспособность продукции (услуг) – $G1$
2	Степень конфиденциальности информации – $G2$
3	Временные характеристики конфиденциальности информации – $G3$
4	ЗИ режимными и организационными методами – $G4$
5	Возможность утечки информации через технические средства – $G5$

Если частная оценка по каждому из пунктов 1–3 равна или больше 20 ($G1 > 20$, $G2 > 20$, $G3 > 20$), то **это подтверждает необходимость проведения мер по защите информации.**

Если частная оценка по каждому из пунктов 4, 5 равна или больше 20 ($G4 > 20$, $G5 > 20$), то это указывает на необходимость проведения ЗИ режимными и организационными методами или с помощью технических

средств защиты соответственно. В том случае, если частная оценка по одному из пунктов 1–3 меньше 20 ($G1 < 20$, $G2 < 20$, $G3 < 20$), то **защиту информации можно не проводить.**

Таким образом, на основе проведенных оценок руководитель организации принимает решение о необходимости проведения работ по организации ЗИ.

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, которая предназначается для определения ориентировочной оценки ожидаемых затрат, связанных с защитой конфиденциальной информации. В общем случае затраты на ЗИ складываются из затрат на проведение организационно-режимных и технических мер. В свою очередь, затраты на техническую защиту складываются из затрат на проведение защиты речевой информации и на защиту других видов информации, в частности, дискретной, обрабатываемой на ПК, телеграфной, факсимильной и других видов, используемых в деятельности организации.

Затраты на режимные и организационные меры ЗИ определяются главным образом заработной платой работников режимных подразделений (групп), обеспечивающих организацию и контроль режимных мер, повышающих безопасность информации. Расчет этих затрат полностью находится в ведении руководителя организации и затруднений не вызывает. Затраты на техническую ЗИ складываются из затрат на проведение исследований, позволяющих выявить каналы утечки информации, определить способы ее защиты, и из ожидаемых затрат на реализацию технических решений защиты.

Порядок выполнения работы

1 Оценить риски информационного объекта по методике *CRAMM*.

2 Согласно идентифицируемым уязвимостям и угрозам в практической работе № 1 определить вероятности их реализации согласно таблицам 3 и 4. Результаты оформить в виде таблицы 5.

3 Осуществить расчет рисков согласно формулам (1), (2).

4 Рассчитать общий риск для всего предприятия по формуле (3).

5 По произведенным расчетам оценить уровень ущерба по таблице 6.

Таблица 3 – **Оценка вероятности осуществления угрозы**

Вероятность атаки	Описание	Значение вероятности
1 Очень низкая	Угроза практически никогда не произойдет	[0; 0,25)
2 Низкая	Маловероятно, что эта угроза осуществится, не существует инцидентов, статистики, мотивов и т.п., которые указывали бы на то, что это может произойти.	[0,25; 0,5)

3 Средняя	Вероятность проведения угрозы равновероятна	0,5
4 Высокая	Возможно, эта угроза осуществится (в прошлом происходили инциденты), или существует статистика или другая информация, указывающая на то, что такие или подобные угрозы иногда осуществлялись прежде, или существуют признаки того, что у атакующего могут быть определенные причины для реализации таких действий	(0,5; 0,75]
5 Очень высокая	Угроза, скорее всего, осуществится. Существуют инциденты, статистика или другая информация, указывающая на то, что угроза, скорее всего, осуществится, или могут существовать серьезные причины или мотивы для атакующего, чтобы осуществить такие действия	(0,75; 1]

Таблица 4 – **Оценка вероятности осуществления угрозы через уязвимости**

Вероятность осуществления	Описание	Значение вероятности
1 Высокая	Уязвимость легко использовать, и существует слабая защита или защита вообще отсутствует	(0,75; 1]
2 Средняя	Уязвимость может быть использована, но существует определенная защита	[0,35; 0,75)
3 Низкая	Уязвимость сложно использовать, и существует хорошая защита	[0; 0,35)

Таблица 5 – **Результаты анализа рисков информационного объекта**

Наименование уязвимости	Наименование угрозы	Вероятность осуществления угрозы	Вероятность осуществления уязвимости	Риск, у.е.

Таблица 6 – **Оценка уровня ущерба**

Уровень ущерба	Описание
1 Малый (менее 1000 у.е.)	Незначительные потери материальных активов, которые быстро восстанавливаются, или незначительные последствия для репутации компании
2 Умеренный (от 1000 до 5000 у.е.)	Заметные потери материальных активов, или умеренные последствия для репутации компании
3 Средней тяжести (от 5000 до 10000 у.е.)	Существенные потери материальных активов или значительный урон репутации компании
4 Большой (от 10000 до 30000 у.е.)	Большие потери материальных активов и большой урон репутации компании

5 Критический (более 30000 у.е.)	Критические потери материальных активов, или полная потеря репутации компании на рынке, что делает невозможным ее дальнейшую деятельность

6 Оценить риски по качественной методике.

7 Используя описание информационной системы ответить на вопросы анкеты (см. приложение А).

8 Рассчитать частные и общие оценки и сделать вывод о необходимости проведения мер по защите информации. Для выполнения работы заполнить таблицу 1.

Содержание отчета

1 Цель работы.

2 Результаты оценки рисков по количественной методике, оформленные согласно таблице 5.

3 Ответы на вопросы анкеты в виде таблицы из приложения А.

4 Результаты оценки рисков по качественной методике, оформленные согласно таблице 1.

5 Вывод по работе.

Контрольные вопросы

1 Этапы количественной методики оценки рисков.
2 Стандарты, регламентирующие управление информационными рисками.
3 Что такое управление информационными рисками?
4 Суть этапа инициализации количественной методики оценки рисков.
5 Критерии оценивания угроз и уязвимостей.
6 Этап анализа рисков.
7 Основные отличия качественной методики оценки рисков от количественной?
8 Этапы качественной методики оценки рисков.
9 Зачем необходимо рассчитывать долевые коэффициенты?
10 Особенность анкетных вопросов в качественной методике оценки рисков.
11 Описание модели безопасности согласно СТБ 34.101.1–2014.
12 Что такое нарушение безопасности.

ПРИЛОЖЕНИЕ А
(*обязательное*)

Анкетные вопросы для качественной методики оценки рисков

№ п/п	Вопросы анкеты	Ответ
	Уровень конкуренции	
1	1 Конкурентоспособна ли Ваша продукция на внутреннем рынке?	
	2 Конкурентоспособна ли Ваша продукция на внешнем рынке?	
	3 Монопольна ли Ваша продукция на внутреннем рынке?	
	Степень конфиденциальности информации, циркулирующей на фирме	
2	1 Имеется ли информация, предназначенная только лицам верхнего звена управления, с грифом «строго конфиденциально»?	
	2 Имеется ли информация, предназначенная ограниченному кругу лиц, выполняющих конкретные операции и задания, в части, их касающаяся, с грифом «конфиденциально»?	
	3 Имеется ли информация ограниченной доступности только работникам организации?	
	Время «старения» конфиденциальности информации	
3	1 Носит ли конфиденциальность долговременный характер (год и более)?	
	2 Носит ли конфиденциальность кратковременный характер (месяц и более)?	
	3 Носит ли конфиденциальность оперативный характер (до месяца)?	
	Режимные и организационные мероприятия	
4	1 Учитываются ли интересы сохранения тайны организации при кадровом отборе верхнего звена управления?	
	2 То же при подборе лиц, допущенных к конфиденциальной информации?	
	3 То же при кадровом отборе штатного персонала организации в целом?	
	4 Налажен ли контроль за сохранением работниками организации коммерческой тайны?	
	5 Обеспечена ли охрана организации и конфиденциальной документации, содержащей коммерческую тайну?	
	6 Возможен ли доступ «недопущенных» лиц к средствам размножения и обработки информации, отнесенной к указанным в пункте 2 категориям конфиденциальности?	
	7 Возможно ли, по Вашему мнению, проникновение агента конкурирующей организации в верхнее звено управления?	
	8 То же в среднее звено управления?	
	9 То же в обслуживающий технику персонал?	
	10 То же в персонал, выполняющий работы, прямо не связанные с конфиденциальной информацией?	
	11 Выделено ли специальное помещение для совещаний и переговоров с деловыми партнерами?	

Окончание приложения А

№ п/п	Вопросы анкеты	Ответ
Оснащение служебных помещений техническими средствами		
5	1 Телефонными аппаратами?	
	2 Переговорными устройствами?	
	3 Датчиками пожарной и охранной сигнализации?	
	4 Электрическими и электронными часами?	
	5 Абонентскими громкоговорителями?	
	6 Телефонными аппаратами с автонабором и концентраторами, используемыми в системах связи?	
	7 Установками прямой телефонной связи?	
	8 Сетевое оборудование?	
	9 Телевизорами?	
	10 Серверами?	
	11 Диктофонами?	
	12 Установкой оперативной (директорской) связи?	
	13 Телефаксами?	
	14 Персональными ЭВМ?	
	15 Видеокамерами?	
	16 Автоматической телефонной станцией?	
	17 Радиотелефоном?	
	18 Организована ли техническая защита на фирме?	

ПРИЛОЖЕНИЕ Б
(*обязательное*)

Долевые коэффициенты для расчета риска по качественной методике

№ п/п	Вопросы анкеты	Долевые коэффициенты оценок	
		общих	частных
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, допущенных 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
	5 Обеспечена ли охрана организации и конфиденциальной документации, содержащей коммерческую тайну?	2,2	7,4

Окончание приложения Б

№ п/п	Вопросы анкеты	Долевые коэффициенты оценок	
		общих	частных
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?	2,2	7,4
Оснащение служебных помещений техническими средствами			
5	1 Телефонными аппаратами?	2,5	8,5
	2 Переговорными устройствами?	1,5	5
	3 Датчиками пожарной и охранной сигнализации?	0,6	2
	4 Электрическими и электронными часами?	0,8	2,5
	5 Абонентскими громкоговорителями?	0,9	3
	6 Телефонными аппаратами с автонабором и концентраторами, используемыми в системах связи?	1,5	5
	7 Установками прямой телефонной связи?	1,3	4,5
	8 Сетевое оборудование?	1,5	5
	9 Телевизорами?	1,5	5
	10 Серверами?	0,5	1,5
	11 Диктофонами?	0,5	1,5
	12 Установкой оперативной (директорской) связи?	1,5	5
	13 Телефаксами?	2,2	7,5
	14 Персональными ЭВМ?	3	10
	15 Видеокамерами?	0,9	3
	16 Автоматической телефонной станцией?	3	10
	17 Радиотелефоном?	1,5	5
	18 Организована ли техническая защита на фирме?	4,5	1,5