Министерство образования Республики Беларусь

Учреждение образования
"Белорусский государственный университет информатики
и радиоэлектроники"

Кафедра защиты информации

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к практическим занятиям по курсам:
"Методы и средства защиты объектов связи
от несанкционированного доступа",
"Защита речевых сообщений и объектов связи
от несанкционированного доступа"

для студентов специальностей:
1-98 01 02 "Защита информации в телекоммуникациях",
1-45 01 03 "Телекоммуникационные системы"
дневной формы обучения

Минск 2008

СОДЕРЖАНИЕ

1. АЛГОРИТМ ОПИСАНИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ 3
2. ОЦЕНКА НЕОБХОДИМОСТИ ЗАЩИТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ**ОШИБКА! ЗАКЛАДКА НЕ**
3. ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 16
4. ИДЕНТИФИКАЦИЯ РИСКОВ 28
5. ОЦЕНКА И УПРАВЛЕНИЕ РИСКАМИ 29
6. АУДИТ БЕЗОПАСНОСТИ 30

1. АЛГОРИТМ ОПИСАНИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Цель работы: Изучить типовой алгоритм описания информационной системы. Получить практические навыки по его применению.

1.1. КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Информационная технология — совокупность методов, способов, приемов и средств обработки документированной информации, включая прикладные программные средства, и регламентированного порядка их применения.

На этапе описания информационной системы (ИС) необходимо указать цели ее создания, ее границы, информационные ресурсы, требования в области информационной безопасности (ИБ) и компонентов управления информационной системой и режимом ИБ.

Описание рекомендуется делать в соответствии со следующим планом:

- аппаратные средства ИС, их конфигурация;
- используемое программное обеспечение (ПО);
- интерфейсы системы, то есть внешние и внутренние связи с позиции информационной технологии;
- типы данных и информации;
- персонал, работающий в данной ИС (обязанности);
- миссия данной ИС (основные цели);
- критичные типы данных и информационные процессы;
- функциональные требования к ИС;
- категории пользователей системы и обслуживающего персонала;
- формальные требования в области информационной безопасности (ИБ), применимые к данной ИС (законодательство, ведомственные стандарты и т.д.);
- архитектура подсистемы ИБ;
- топология локальной сети;
- программно-технические средства обеспечения ИБ;
- входные и выходные потоки данных;
- система управления в данной ИС (должностные инструкции, система планирования в сфере обеспечения ИБ);

- существующая система управления в области ИБ (резервное копирование, процедуры реагирования на нештатные ситуации, инструкции по ИБ, контроль поддержания режима ИБ и т.д.);
- организация физической безопасности;
- управление и контроль внешней по отношению к ИС средой (климатическими параметрами, электропитанием, защитой от затоплений, агрессивной среды и т.д.).

Для системы, находящейся в стадии проектирования, и для уже существующей системы характер описания и степень подробности ответов будут разными. В первом случае (стадия проектирования) достаточно указать общие требования в области ИБ.

Технология описания системы

Для получения информации по перечисленным пунктам на практике рекомендуется использовать:

- разнообразные вопросники (check-листы), которые могут быть адресованы к различным группам управленческого и обслуживающего персонала;
- интервью аналитиков (внешних), которые проводят неформальные беседы с персоналом и затем готовят формализованное описание;
- анализ формальных документов и документации предприятия;
- специализированный инструментарий (ПО).

Существует ПО, благодаря которому удается частично автоматизировать процесс описания. К нему относятся: сканеры, дающие возможность составить схему информационной системы, программы для структурированного описания информационных систем, позволяющие создать необходимые отчетные формы.

1.2. ЗАДАНИЕ

1. Создать компанию, деятельность которой - сфера информационных технологий;

2. Конкретизировать род деятельности компании, определить ее штат, структуру административного управления;

3. Составить краткие должностные инструкции (в части обязанностей) для каждой категории работников компании;

4. Категорировать информацию, с которой работают в данной компании исходя из ее рода деятельности.

5. Составить полный список необходимого оборудования, для нормальной работы компании включая, при необходимости, и бытовую технику;

6. Составить схему информационной системы компании с учетом соответствующего оборудования;

1.3. СОДЕРЖАНИЕ ОТЧЕТА

1. Цель работы.
2. Результаты выполнения задания.
3. Вывод по работе.

2. ОЦЕНКА НЕОБХОДИМОСТИ ЗАЩИТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Цель работы: Изучить методики оценки необходимости защиты информационной системы и определения ожидаемых затрат на защиту информации. Получить практические навыки по их применению.

2.1. 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 ЗИ от перехвата ее техническими средствами и агентами конкурентов весьма актуальна как для государственного, так и негосударственного сектора. Особенно остро в настоящее время встает вопрос о необходимости защиты конфиденциальной информации негосударственного сектора. Это обусловлено тем, что государственный сектор давно серьезно занимался ЗИ и имеет в настоящее время 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 все стороны деятельности организации, связанные с циркулирующей на 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 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 на фирме, 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 табл. 1. Ответы на вопросы анкеты в форме «да» или «нет» заносятся в графу 3 против соответствующих вопросов (см. табл. 2.)

На втором этапе с привлечением консультанта проводится анализ результатов опроса. Если ответ на вопрос соответствует увеличению опасности утечки информации, то в графе 4 табл. 3 проставляется знак «+», в противном случае проставляется знак «-».

Таблица 1

Перечень вопросов анкеты

№ п/п	Вопросы анкеты	Долевые коэффициенты для общих оценок	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

Продолжение таблицы 1

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
	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

Продолжение таблицы 1

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
	б) Телефонными аппаратами с автонабором и концентраторами, используемыми в системах связи?	1,5	5
	7) Установками прямой телефонной связи?	1,3	4,5
	8) Радиоприемниками?	1,5	5
	9) Телевизорами?	1,5	5
	10) Магнитофонами?	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) Видеомагнитофонами?	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

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 на фирме в Целом. При этом если общая оценка G равна или больше 50 (G>50), то **защиту необходимо проводить по всем направлениям.**

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	1	да	+	3.5	35		35
	2	нет	-	5	50		
	3	нет	-	1.5	15		
2	1	да	+	11	55		100
	2	да	+	5	25		
	3	да	+	4	20		
3	1	да	+	5	50		90
	2	да	+	4	40		
	3	нет	-	1	10		
4	1	да	+	3.8	13		49.6
	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	19.7		
	8	нет	-	37	12.3		
	9	да	+	2.3	7.6		
	10	Да	+	1.5.	5		
	11	нет	-	2.2	7.4		
5	1	да	+	2.5	8.5		28
	2	да	+	1.5	5		
	3	да	+	0.6	2		
	4	да	+	0.8	2.5		
	5	нет	-	0.9	3		
	6	да	+	15	5		
	7	нет	-	1.3	4.5		
	8	да	+	1.5	5		

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 дополнительную защиту информации можно не проводить.**

На четвертом этапе проводится анализ с помощью частных оценок по всем 5 пунктам опросной анкеты. Для получения частных оценок проводят суммирование долевых коэффициентов графы 6 табл. 2, помеченных знаком «+» для каждого пункта 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 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.**

Если частная оценка по каждому из пунктов 4, 5 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 по одному из пунктов 1-3 меньше 20 (G 1, 2, 3 < 20), то **ЗИ 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.

Вторая часть методики 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.

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, разработана и представлена ниже. Учитывая, что методика предназначена для проведения экспресс-оценки стоимости ЗИ, позволяющей руководителю организации грубо оценить предстоящие затраты, она максимально упрощена и предусматривает проведение элементарных расчетов. С этой целью все техническое оборудование, которое может быть установлено на объекте (фирме) и через которое возможна утечка информации, условно разделено на три группы. Критерием такого деления выбрана доля (процент) затрат на защиту оборудования от стоимости самого оборудования (техники). Долевые коэффициенты (Kl, К2, КЗ) определены экспертным путем и приведены в табл. 3.

Таблица 3

Стоимость защиты оборудования

Группа	Перечень оборудования	Доля (процент) затрат на защиту оборудования от утечки информации	Доля (процент) затрат на профилактический ежегодный контроль эффективности ЗИ
1	Телефонные аппараты, переговорные устройства, датчики пожарной и охранной сигнализации, электрические электронные часы, абонентские громкоговорители;	$K_1 = 0,7 \cdot C_1$	$K_{проф} = (0,1 \div 0,05) \cdot (C_1 + C_2 + C_3)$
2	Автонаборы и концентраторы, используемые в системах связи; установки прямой телефонной связи; радиоприемники; телевизоры; магнитофоны; диктофоны	$K_2 = 0,3 \cdot C_2$	
3	Пульты оперативной (директорской) связи до 100 номеров; персональная компьютерная техника, видеомагнитофоны; АТС на 100-1000 номеров	$K_3 = 0,15 \cdot C_3$	

Перечень технического оборудования по группам с указанием значений долевых коэффициентов затрат на защитные мероприятия приведен в табл. 3. В таблице обозначено: С 1, 2, 3 — суммарная стоимость технического оборудования соответствующей группы, установленного на объекте. Значения стоимости образцов техники, находящихся в помещениях организации, определяются по каталогам действующих цен изготовителя данной техники. Стоимость технической защиты всего оборудования ($С_{тз}$), состоящего из техники различных групп, определяется по формуле:

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

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

Стоимость ежегодного профилактического контроля определяется по формуле:

$$C_{проф} = K_{проф} \qquad (2)$$

где $К_{проф}$=0,05-0,1 — коэффициент затрат на ежегодный профилактический контроль эффективности ЗИ, определенный опытным путем.

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

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

где $С_{общ.з.}$ - общие затраты на ЗИ; $С_{роз}$ - затраты на режимные и организационные меры.

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

2.2. ЗАДАНИЕ

1. Используя описание информационной системы ответить на вопросы анкеты (таблица 1);

2. Провести оценку защиты информационной системы в соответствии с методикой;

3. Оценить ожидаемые затраты на обеспечение безопасности информационной системы;

2.3. СОДЕРЖАНИЕ ОТЧЕТА

1. Цель работы.
2. Результаты выполнения задания.
3. Вывод по работе.

3. ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цель работы: Сформулировать задачи и обеспечить поддержку мер в области информационной безопасности со стороны руководства организации.

3.1. КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Кому и что доверять

От правильного выбора уровня доверия к сотрудникам зависит успех или неудача реализации политики безопасности компании. При этом слишком большой уровень доверия может привести к возникновению проблем в области безопасности, а слишком малый — заметно затруднить работу сотрудника, вызвать у него недоверие и даже привести к увольнению. Обычно используют следующие модели доверия:

доверять всем и всегда — самая простая модель доверия, но непрактичная;

не доверять никому и никогда — самая ограниченная модель доверия и также непрактичная;

доверять избранным на время — модель доверия подразумевает определение разного уровня доверия на определенное время. При этом доступ к информационным ресурсам компании предоставляется по необходимости для выполнения служебных обязанностей, а средства контроля доступа используются для проверки уровня доверия к сотрудникам компании.

Трудности внедрения политик безопасности

Опыт создания политик безопасности показывает, что внедрение политики безопасности часто приводит к возникновению напряженности во взаимоотношениях между сотрудниками компании. Это в основном связано с тем, что сотрудники часто стараются не следовать каким-либо правилам безопасности, так как не хотят себя ограничивать в своих действиях. Другая причина в том, что каждый сотрудник имеет свое представление (не обязательно солидарное с принятой в компании политикой безопасности) о необходимости и способах организации режима информационной безопасности в компании. Например, сотрудники контура сбыта заинтересованы в оперативном исполнении своих обязанностей без каких-либо задержек, связанных с применением средств защиты информации. Персонал службы поддержки часто заинтересован только в

простоте эксплуатации администрируемых ими информационных систем. TOP-менеджмент компании заинтересован прежде всего в оптимизации затрат и уменьшении общей стоимости владения (TCO) корпоративной системы защиты информации. Получить одобрение всех положений политики безопасности у перечисленных групп сотрудников компании — трудная и практически неосуществимая задача. Поэтому лучше всего попробовать достигнуть некоторого компромисса.

Кто заинтересован в политиках безопасности

Политики безопасности затрагивают практически каждого сотрудника компании. Сотрудники службы поддержки будут осуществлять и поддерживать правила безопасности компании. Менеджеры заинтересованы в обеспечении безопасности информации для достижения своих целей. Юристы компании и аудиторы заинтересованы в поддержании репутации компании и предоставлении определенных гарантий безопасности клиентам и партнерам компании. Рядовых сотрудников компании политики безопасности затрагивают больше всего, поскольку правила безопасности накладывают ряд ограничений на поведение сотрудников и затрудняют выполнение работы.

Состав группы по разработке политик безопасности

Буклет SAGE «A Guide to Developing Computing Policy Documents» рекомендует следующий: состав рабочей группы по разработке политик безопасности:

- член совета директоров;
- представитель руководства компании (CEO, финансовый директор, директор по развитию);
- СЮ (директор службы автоматизации);
- CISO (директор по информационной безопасности);
- аналитик службы безопасности;
- аналитик ИТ-службы;
- представитель юридического отдела;
- представитель от пользователей;
- технический писатель.

Численность группы по разработке политик безопасности будет зависеть от широты и глубины проработки политик безопасности. Например, разработка

политик безопасности для офисной сети в 40-50 узлов может занять один человекомесяц.

Процесс разработки политик безопасности

Если это возможно, то о том, что разрабатывается новая политика информационной безопасности компании, необходимо уведомить сотрудников заранее. До начала внедрения новой политики безопасности желательно предоставить сотрудникам текст политики на одну-две недели для ознакомления и внесения поправок и комментариев. Также надо учитывать, что без прав нет обязанностей то есть сотрудники, на которых распространяются правила безопасности, должны обладать всеми необходимыми полномочиями для того, чтобы выполнять эти правила.

Основные требования к политике безопасности

В идеале политика безопасности должна быть реалистичной и выполнимой, краткой и понятной, а также не приводить к существенному снижению общей производительности бизнес-подразделений компании. Политика безопасности должна содержать основные цели и задачи организации режима информационной безопасности, четкое описание области действия, а также указывать на ответственных и их обязанности. Например, по мнению специалистов Cisco, желательно, чтобы описание политики безопасности занимало не более двух (максимум пяти) страниц текста. При этом важно учитывать, как политика безопасности будет влиять на уже существующие информационные системы компании. Как только политика утверждена, она должна быть представлена сотрудникам компании для ознакомления. Наконец, политику безопасности необходимо пересматривать ежегодно, чтобы отражать текущие изменения в развитии бизнеса компании.

Уровень средств безопасности

Хорошо написанные политики безопасности компании должны позволять балансировать между достигаемым уровнем безопасности и получаемым уровнем производительности корпоративных информационных систем компании. Одна из основных целей политики безопасности состоит в том, чтобы обосновать и внедрить средства защиты информации, адекватные целям и задачам бизнеса. Выбор необходимых средств защиты информации для определенной политики безопасности не всегда понятен и легко определяем. Здесь решающую роль играют необходимость организации режима информационной

безопасности, а также бизнес-культура компании. При этом если правила политики безопасности слишком ограничительны или слишком жестки, для того чтобы их внедрять и соответствовать им в дальнейшем, то либо они будут игнорироваться, либо сотрудники компании найдут способ обойти средства безопасности.

Примеры политик безопасности

В настоящее время ряд ведущих компаний в области безопасности выделяют следующие политики:

- допустимого шифрования,
- допустимого использования,
- аудита безопасности,
- оценки рисков,
- классификации данных,
- управления паролями,
- использования ноутбуков,
- построения демилитаризованной зоны (DMZ),
- построения экстранет,
- безопасности рабочих станций и серверов,
- антивирусной защиты,
- безопасности маршрутизаторов и коммутаторов,
- безопасности беспроводного доступа,
- организации удаленного доступа,
- построения виртуальных частных сетей (VPN) и пр.,
- безопасности периметра.

3.2. ПОЛИТИКИ БЕЗОПАСНОСТИ, РЕКОМЕНДУЕМЫЕ SANS

Институт SANS подготовил ряд политик безопасности, которые можно найти на сайте института (www.sans.org) К ним относятся:

1. политика допустимого шифрования,
2. политика допустимого использования,
3. руководство по антивирусной защите,
4. политика аудита уязвимостей,
5. политика хранения электронной почты,
6. политика использования электронной почты компании,
7. политика использования паролей,

8. политика оценки рисков,
9. политика безопасности маршрутизатора,
10. политика обеспечения безопасности серверов,
11. политика виртуальных частных сетей,
12. политика беспроводного доступа в сеть компании,
13. политика автоматического перенаправления электронной почты компании,
14. политика классификации информации,
15. политика в отношении паролей для доступа к базам данных,
16. политика безопасности лаборатории демилитаризованной зоны,
17. политика безопасности внутренней лаборатории,
18. политика экстранета,
19. политика этики,
20. политика лаборатории антивирусной защиты.

1. Политика допустимого шифрования

Цель

Основной задачей этой политики является определение разрешенных к использованию алгоритмов шифрования. Политика обеспечивает гарантии соблюдения федеральных законов и юридического разрешения для распространения и использования технологий шифрования за пределами США.

Область действия

Политика обязательна для всех сотрудников компании.

Суть политики

Для шифрования должны быть использованы испытанные стандартные алгоритмы типа DES, Blowfish, RSA, RC5 и IDEA. Эти алгоритмы могут быть использованы в приложениях, разрешенных к применению в компании. Например, PGP производства NAI применяет комбинацию IDEA и RSA или Diffie-Hellman, в то время как SSL — шифрование RSA. Ключи для симметричного шифрования должны иметь длину как минимум 56 бит. Ключи для асимметричного шифрования должны иметь длину, соответствующую аналогичной стойкости. Требования к длине ключей должны пересматриваться в компании ежегодно.

Использование других алгоритмов шифрования разрешено, если это рекомендовано квалифицированной группой экспертов и получено разрешение отдела информационной безопасности. Экспорт технологий шифрования за

пределы США ограничен экспортными законами. Резиденты за пределами США, использующие шифрование, обязаны ориентироваться на законы стран, в которых они находятся.

Ответственность

К любому сотруднику, нарушившему эту политику, могут быть применены дисциплинарные меры, вплоть до увольнения.

Термины и определения

Симметричное шифрование — метод шифрования, при котором один и тот же ключ используется и для шифрования, и для дешифрования.

Асимметричное шифрование — метод шифрования, при котором один ключ используется для шифрования, а другой — для дешифрования.

2. Политика допустимого использования

Основной задачей издания этой политики отделом информационной безопасности является не наложение ограничений на установленную в компании культуру открытости, доверия и целостности, а защита сотрудников и партнеров компании от преднамеренных и непреднамеренных противоправных действии со стороны других людей. Системы компании, связанные с Интернетом/интранетом/экстранетом, включая компьютерное оборудование, программное обеспечение, операционные системы, системы хранения данных, учетные записи для доступа к электронной почте, к Web-ресурсам, являются собственностью компании. Эти системы должны использоваться только с деловой целью в интересах компании и ее клиентов.

Цель

Цель этой политики состоит в определении допустимого использования компьютерного оборудования в компании. Эти правила предназначены для защиты компании и ее сотрудников, чтобы не подвергать их рискам, включая вирусные атаки, взлом систем, и не допускать возникновения юридических проблем.

Область действия

Политика обязательна для всех сотрудников, подрядчиков, консультантов, временных сотрудников и других работающих в компании, включая весь персонал сторонних компаний, пользующихся информационными системами или оборудованием компании. Положения этой политики относятся и ко всему оборудованию, которое является собственностью компании или взято ею в аренду.

Суть политики

Общие вопросы использования и владения:

- администраторы корпоративной сети стремятся обеспечить разумный уровень конфиденциальности передаваемых сотрудниками данных, а сотрудники должны знать, что данные, которые они создают в корпоративных системах, являются собственностью компании. Из-за необходимости обеспечения безопасности корпоративной сети компании, руководство не может гарантировать конфиденциальность информации, хранимой на любом устройстве сети, принадлежащем компании;
- сотрудники ответственны за использование ресурсов компании в личных целях. Отделы ответственны за создание руководящих документов по использованию ресурсов компании в личных целях. При отсутствии таких политик сотрудникам следует руководствоваться требованиями и положениями политик более высокого уровня, в случае возникновения вопросов необходимо обращаться к своему непосредственному начальнику;
- отдел информационной безопасности рекомендует, чтобы любая информация, которую сотрудники считают важной, была зашифрована. В качестве руководства по классификации информации и ее защите используйте политику по защите информации отдела информационной безопасности. По вопросам шифрования сообщений электронной почты и документов используйте ознакомительные программы, разработанные отделом информационной безопасности;
- в соответствии с политикой аудита уязвимостей, определен список людей, имеющих право мониторинга оборудования, информационных систем и сетевого трафика в любое время;
- компания имеет право периодически проводить аудит корпоративной сети и информационных систем для проверки выполнения этой политики.

Безопасность и конфиденциальная информация компании:

- пользовательские интерфейсы для доступа к корпоративной информации должны быть классифицированы как конфиденциальные или не конфиденциальные в соответствии с руководящими

документами по вопросам конфиденциальности, которые находятся в отделе кадров. Конфиденциальной информацией могут быть списки клиентов, планы стратегического развития, торговые секреты и т.д. Сотрудники должны принять все необходимые меры, чтобы предотвратить неправомочный доступ к этой информации;

- сотрудники компании ответственны за безопасность их паролей и учетных записей. Пароли системного уровня должны изменяться один раз в квартал, пароли учетных записей сотрудников должны изменяться раз в шесть месяцев;
- при появлении у сотрудника необходимости оставить рабочее место без присмотра все серверы, портативные компьютеры и автоматизированные рабочие места должны быть защищены включением скринсейвера с паролем, активирующимся после 10 или менее минут бездействия, или путем выхода из системы (logging-off);
- шифрование используется в соответствии с политикой допустимого шифрования отдела информационной безопасности;
- поскольку информация, содержащаяся в портативных компьютерах, более уязвима, необходимо предпринимать усиленные меры безопасности;
- при использовании корпоративной электронной почты сотрудники должны указывать, что выраженные ими мнения являются только их собственными и не представляют собой точку зрения компании, кроме случаев, когда они выполняют при этом свои деловые обязанности;
- все компьютеры, используемые сотрудниками для доступа к ресурсам компаний, независимо от того, являются они собственностью компании или принадлежат сотруднику, должны иметь утвержденное отделом безопасности информации антивирусное программное обеспечение с самой последней базой обновлений;
- сотрудники должны быть особенно внимательны при открытии вложений в сообщениях электронной почты, полученных от неизвестных отправителей, так как они могут содержать вирусы, почтовые «бомбы» или программы типа «Троянский конь».

Запрещается! Список, представленный ниже, не является исчерпывающим, но здесь сделана попытка определить действия, которые попадают в категорию запрещенных:

В сфере действий в корпоративной сети:

- нарушения прав любого человека или компании, защищенных авторским правом, законами о торговых секретах, патентами или другим законом о защите интеллектуальной собственности, включая установку или распространение «пиратского» или другого программного обеспечения, которые не лицензировано для использования в компании;
- неправомочное копирование защищенного авторским правом материала, включая преобразование в цифровую форму и распространение фотографий из журналов, книг или других защищенных авторским правом источников, музыки и установка любого защищенного авторским правом программного обеспечения, для которого компания или данный сотрудник не имеют действующей лицензии;
- экспорт программного обеспечения, технической информации, программного обеспечения по шифрованию данных или технологии в нарушение международных или региональных экспортных законов. Перед экспортированием любого материала руководство должно проконсультироваться с соответствующими органами;
- запуск злонамеренных программ в сети или на компьютере (например, вирусов, «червей», «Троянских коней», почтовых «бомб», и т.д.);
- разглашение ваших паролей другим сотрудникам или разрешение пользоваться кому-либо вашей учетной записью или паролями. Сюда относятся и члены семьи, если работа выполняется дома;
- использование корпоративных ресурсов для создания, передачи или хранения материалов сексуального, религиозного и другого характера, не относящихся к выполнению служебных обязанностей;
- мошеннические предложения изделий, продуктов или услуг с использованием учетной записи пользователя компании;
- создание заявления о гарантиях, явных или подразумеваемых, если это не является частью обязанностей при выполнении работы;
- нарушение безопасности корпоративной сети: получение доступа к данным, к которым сотрудник не должен его иметь; регистрация на ресурсах, к которым сотруднику явно не разрешен доступ; про-

слушивание сетевого трафика; выполнение различных атак на ресурсы компании и т.д.;

- сканирование портов или поиск уязвимостей, если на это не получено разрешение от отдела информационной безопасности;
- выполнение любой формы мониторинга сети с перехватом данных, не направленных на компьютер сотрудника, если эта деятельность не является частью его обязанностей;
- попытки обхода систем установления подлинности или безопасности приложений, операционных систем и оборудования;
- попытки ограничения доступа сотрудников к корпоративным ресурсам, за исключением компьютера сотрудника;
- использование программ/скриптов/команд или отправки сообщений любого вида с намерением ограничить доступ или разорвать сессию другого сотрудника;
- разглашение списка сотрудников компании сторонним организациям или лицам;

В сфере, связанной с передачей информации в электронном виде:

- посылка сообщений электронной почты с незапрашиваемой получателем информацией (junk-mail) или рекламного материала кому-либо без его просьбы (спам электронной почты);
- любая форма преследования через электронную почту, телефон или пейджер;
- неправомерное использование или подделывание заголовков почтовых сообщений;
- подслушивание сообщений электронной почты других сотрудников;
- создание или отправление «цепочек писем» или других писем по схеме типа «пирамида»;
- использование электронной почты других поставщиков интернет-услуг для рекламирования услуг и продуктов своей компании;
- отправка не относящихся к бизнесу сообщений большому количеству участников новостных групп (спам новостных групп).

Ни при каких обстоятельствах сотрудник компании не должен участвовать в любой деятельности, которая является незаконной по местным, феде-

ральным или международным законам с использованием средств и ресурсов компании.

Ответственность

К любому сотруднику, нарушившему эту политику, могут быть применены дисциплинарные меры, вплоть до увольнения.

Термины и определения

Спам — неразрешенные и/или незапрашиваемые массовые отправки электронных почтовых сообщений.

3.3. СОДЕРЖАНИЕ ОТЧЕТА

1. Цель работы.
2. Результаты выполнения задания.
3. Вывод по работе.

4. ИДЕНТИФИКАЦИЯ РИСКОВ

Цель работы: Изучить типовой алгоритм описания информационной системы. Получить практические навыки по его применению.

5. ОЦЕНКА И УПРАВЛЕНИЕ РИСКАМИ

Цель работы: Изучить типовой алгоритм описания информационной системы. Получить практические навыки по его применению.

6. АУДИТ БЕЗОПАСНОСТИ

Цель работы: Изучить типовой алгоритм описания информационной системы. Получить практические навыки по его применению.

ЛИТЕРАТУРА

1. Петренко С.А. Курбатов В.А. Политики информационной безопасности. М.: Компания АйТи, 2006. – 400 с.

2. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность. М.: Компания АйТи; ДМК Пресс, 2005. – 485 с.