Федеральное государственное автономное образовательное
учреждение высшего образования
«СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ РАДИОЭЛЕКТРОНИКИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Кафедра «Информационная безопасность»

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ И ПРОГНОЗИРОВАНИЕ ИНФОРМАЦИОННЫХ УГРОЗ

Часть 1

АНАЛИЗ ИНФОРМАЦИОННЫХ РИСКОВ

Учебно-методическое пособие
для обучающихся по направлению
10.04.01 «Информационная безопасность»

Севастополь
СевГУ
2018

УДК 004.056.5(075.8)
ББК 32.81я73
М34

Р е ц е н з е н т:
Л.В. Третьякова – д.ф.-м.н., профессор кафедры ВМ института ИТиУТС

Составители: М.А. Маслова, И.П. Шумейко

М34 Математическое моделирование и прогнозирование информационных угроз: учеб.-метод. пособие для обучающихся по направлению 10.04.01 «Информационная безопасность» (уровень подготовки – магистр) очной и очно-заочной форм обучения. – Ч. 1. Анализ информационных рисков / Сост. М.А. Маслова, И.П. Шумейко. – Севастополь: СевГУ, 2018. – 60 с.

В пособии рассмотрены методические указания к практическим работам раздела «Анализ информационных рисков» по дисциплине «Математическое моделирование и прогнозирование информационных угроз».

Данное пособие может быть использовано для самостоятельной практической подготовки студентов очной и очно-заочной форм обучения направления подготовки 10.04.01 «Информационная безопасность» (профиль: «Организация и технология защиты информации»).

УДК 004.056.5(075.8)
ББК 32.81я73

Рассмотрено и утверждено методической комиссией института радиоэлектроники и информационной безопасности СевГУ, протокол № 6 от 25 мая 2018 г.

Допущено учебно-методическим центром СевГУ в качестве учебно-методического пособия.

© ФГАОУ ВО «Севастопольский государственный университет», 2018

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Основой управления информационной безопасностью организации является анализ рисков, что особо отмечено в международных и российских стандартах в сфере безопасности информационных технологий и систем менеджмента информационной безопасности (ГОСТ Р ИСО/МЭК 27001-2006). В организациях, в которых обращается информация, составляющая государственную тайну, процесс создания систем управления информационной безопасностью заключается в удовлетворении нормативным требованиям с применением специального оборудования, программного обеспечения и привлечением специализированных организаций. В коммерческих предприятиях, в которых циркулирует информация, составляющая коммерческую и профессиональную тайны, а также персональные данные, процесс построения таких систем должен основываться на анализе рисков.

Фактически риск представляет собой интегральную оценку того, насколько эффективно существующие средства защиты способны противостоять информационным угрозам. Другими словами, риск можно определить как функцию вероятности реализации определенной угрозы (использующей некоторые уязвимости) и величины возможного ущерба.

Анализ рисков рассматривают как процесс идентификации информационных рисков, определение вероятности их осуществления и потенциального воздействия, а также имеющихся контрмер, уменьшающих это воздействие (угроз и уязвимостей). В свою очередь управление рисками включает анализ рисков, выбор, реализацию и оценку эффективных и экономичных контрмер, проверку адекватности установленного уровня приемлемого риска. При этом важным условием является непрерывность и своевременность осуществления процедур управления рисками на каждом из этапов жизненного цикла информационной системы (ИС).

Таким образом, качественно организованный процесс анализа рисков позволяет на основе оценки критичных областей, отрицательно влияющих на ключевые бизнес-процессы компании выработать эффективные и обоснованные решения для контроля или минимизации выявленных рисков, определения баланса между возможным ущербом от утечки информации и размерами затрат на ИБ с наглядным представлением структуры этих затрат для руководства.

Выделяют две основные группы методов расчёта рисков информационной безопасности. Методы первой группы позволяют установить уровень риска путём оценки степени соответствия определённому набору требований по обеспечению информационной безопасности. В качестве источников таких требований могут выступать: требования действующего российского законодательства; нормативно-правовые документы предприятия, касающиеся вопросов информационной безопасности; рекомендации международных стандартов; рекомендации компаний-производителей программного и аппаратного обеспечения и др.

Вторая группа методов оценки рисков информационной безопасности базируется на определении вероятности реализации угроз, а также уровней их ущерба. В данном случае значение риска вычисляется отдельно для каждой атаки и в общем случае представляется как произведение вероятности проведения атаки на величину возможного ущерба от этой атаки. Значение ущерба определяется собственником информационного ресурса, а вероятность атаки вычисляется группой экспертов, проводящих процедуру аудита.

Методы первой и второй группы могут использовать количественные или качественные шкалы для определения величины риска информационной безопасности. В первом случае риск и все его параметры выражаются в числовых значениях. При использовании количественных шкал вероятность реализации угрозы может выражаться числом в интервале, а ущерб может задаваться в виде денежного эквивалента материальных потерь, которые может понести организация в случае успешного проведения атаки. При использовании качественных шкал числовые значения заменяются на эквивалентные им понятийные уровни. Каждому понятийному уровню в этом случае будет соответствовать определённый интервал количественной шкалы оценки. Количество уровней может варьироваться в зависимости от применяемых методик оценки рисков.

При расчете значений вероятности проведения атаки, а также уровня возможного ущерба могут использоваться статистические методы, методы экспертных оценок или элементы теории принятия решений. Статистические методы предполагают анализ уже накопленных данных о реально случавшихся инцидентах, связанных с нарушением информационной безопасности. На основе результатов такого анализа строятся предположения о вероятности реализации угроз и уровнях ущерба от них в других информационных системах. Однако применение статистических методов не всегда возможно из-за отсутствия в полном объёме статистических данных о ранее проведённых атаках на информационные ресурсы ИС, аналогичной той, которая выступает в качестве объекта оценки.

При использовании аппарата экспертных оценок проводится анализ результатов работы группы экспертов, компетентных в области информационной безопасности, которые на основе имеющегося у них опыта определяют количественные или качественные уровни риска. Элементы теории принятия решений позволяют применять для вычисления значения риска безопасности более сложные алгоритмы обработки результатов работы группы экспертов.

Существует большое количество методик оценки рисков, которые различаются степенью детализации, требованиями к подготовке персонала и вовлекаемыми ресурсами. Однако в качестве основных требований, предъявляемых к таким методикам, можно выделить следующие: эффективность применения полученных результатов для создания системы управления информационной безопасностью, приемлемое количество исходных данных, однозначно трактуемые выходные результаты.

Основными вопросами, соответствующими этапам анализа рисков, при этом остаются:

– что мы хотим защитить и почему? При этом проводится описание информационной системы, идентификация активов и их классификация с позиции ценности;

– от чего мы хотим защититься? Этот этап подразумевает идентификацию угроз и незакрытых уязвимостей и их ранжирование, организация защиты информации;

– какова вероятность возникновения и успешной реализации угрозы? Вероятности угроз определяются при существующей инфраструктуре ИТ;

– что мы потеряем, если угроза будет успешно реализована? Проводится оценка возможного ущерба;

– оценка риска (по отдельным угрозам, классам угроз, интегральный риск по организации).

В процессе анализа рисков информационной безопасности могут использоваться специализированные программные комплексы, позволяющие автоматизировать процесс анализа исходных данных и расчёта значений рисков. В частности, разработаны системные утилиты или программное обеспечение для оценки рисков, утилиты для моделирования угроз и уязвимостей, существует программное обеспечение и шаблоны документов для проведения оценки и определения мероприятий по защите информации.

В данном пособии рассмотрены практические работы, направленные на формирование практических навыков использования основного инструментария оценки информационных рисков, применения специальных методик и программного обеспечения, а именно: идентификация и оценки рисков, обоснование рисковых решений методом «дерева решений», анализ рисков информационной безопасности на основе модели угроз и уязвимостей, расчет информационных рисков согласно методикам RiskWatch, CORAS и др.

Практическая работа № 1
ИДЕНТИФИКАЦИЯ И ОЦЕНКА РИСКОВ

Цель работы – формирование навыков проведения групповой экспертизы на примере формирования листа 10 важнейших рисков.

Ход выполнения работы

1. Работа выполняется подгруппами по 3 – 5 чел.
2. Студентам выдается задание, которое они изучают в течение 3 – 5 мин (Приложение А)
3. Оформляется заголовок отчета по практической работе. Бланк отчета смотреть в Приложении А.
4. По подгруппам методом мозгового штурма применительно к своему варианту уточняются предложенные критерии оценки значимости мнений экспертов, формулируется один свой собственный критерий и разрабатывается шкала для оценки экспертов по этому критерию. Результаты заносятся в отчет.
5. Каждый эксперт оценивает важность критериев из предыдущего пункта (включая сформулированный), ранжируя их в порядке убывания значимости: 1-й – самый важный, последний – наименее важный. Каждым индивидуально заполняется оценочная таблица 1.1 – у каждого эксперта свои собственные оценки.
6. Мнения экспертов обобщаются в таблице 1.2 – совпадает у всех экспертов: первые строки таблицы переносятся из таблиц 1.1, заполненных экспертами индивидуально, затем в следующей строке рассчитывается сумма рангов критериев – по столбцам, – и их общая сумма, в следующей строке выполняется вспомогательный расчет: общая сумма рангов делится на сумму рангов каждого критерия (число из последнего столбца предыдущей строки на число соответствующего столбца предыдущей строки), а затем полученные значения складываются; в последней строке приводится результат деления соответствующего числа вспомогательной строки на сумму значений из вспомогательной строки. Точность расчетов – 2 знака после запятой.
7. Каждый эксперт самостоятельно по критериям, используя разработанные шкалы, оценивает всех членов экспертной группы, включая себя, заполняя таблицу 1.3.
8. Оценивается значимость мнений каждого эксперта – ранг эксперта. Для этого заполняется таблица 1.4, одинаковая для всех в подгруппе: сначала по каждому эксперту заносятся в соответствующие строки суммы выставленных баллов по каждому из критериев, затем рассчитываются средневзвешенные баллы, их сумма, а в следующем столбце – отношение средневзвешенного балла к сумме баллов с точностью до 2 знаков после запятой.

9. Каждый эксперт самостоятельно письменно предлагает 5 – 7 рисков, которым следовало бы уделить внимание в данной ситуации, затем риски обсуждаются, несущественные риски отбрасываются, формулируется общий список. «Свои» риски отделяются от рисков, предложенных другими членами группы, горизонтальной линией. Каждому риску присваивается свой единый для всех экспертов код (чтобы впоследствии сэкономить время на заполнение таблиц). Для анализа должен быть составлен список из 15 – 20 рисков.

10. Совместно методом мозгового штурма в подгруппах применительно к своему конкретному заданию уточняются предложенные критерии оценки важности рисков и формулируется один свой собственный. Результаты заносятся в отче.

11. Каждый эксперт оценивает важность критериев из предыдущего пункта (включая сформулированный), ранжируя их в порядке убывания значимости: 1-й – самый важный, последний – наименее важный. Каждым индивидуально заполняется оценочная таблица 1.6 – у каждого эксперта свои собственные оценки.

12. Оценивается значимость каждого критерия – вес критерия. Для этого заполняется таблица 1.7, одинаковая для всех в подгруппе: сначала по каждому эксперту заносятся в соответствующие строки суммы выставленных рангов по каждому из критериев, затем рассчитываются средневзвешенные ранги по каждому из критериев – по столбцам, их сумма, в следующей строке – отношение суммы средневзвешенных рангов к соответствующему средневзвешенному рангу, а затем – следующей строке вес критерия, как отношение соответствующего значения из предыдущей строки к сумме вспомогательных значений предыдущей строки. Точность расчетов – 2 знака после запятой.

13. Каждый эксперт самостоятельно оценивает важность критериев рисков с точки зрения каждого из предложенных критериев, ранжируя их в порядке убывания значимости: 1-й – самый важный, последний – наименее важный. Каждым индивидуально заполняется оценочная таблица 1.8 – у каждого эксперта свои собственные оценки. Затем рассчитывается средневзвешенный ранг риска и окончательный ранг (число в скобках в последнем столбце) – порядковый номер при расположении рисков в порядке возрастания рангов.

14. Формируется обобщенный лист 10 важнейших рисков. Для этого заполняется таблица 1.8, одинаковая для всех в подгруппе: сначала по каждому эксперту заносятся в соответствующие столбцы выставленные ранги по каждому из рисков (последние столбцы таблицы 1.8 – значения в скобках), а затем рассчитываются средневзвешенные ранги по каждому из рисков – по строкам. Точность расчетов – 2 знака после запятой Рассчитанные ранги ранжируются в порядке возрастания и нумеруются (число в скобках). Первые 10 рисков включаются в лист 10 важнейших рисков, который завершает отчет о данной практической работе.

Пример выполнения задания приводится ниже.

Пример отчета

ООО «КапраЛ» было недавно зарегистрировано как предприятие по выпуску товаров народного потребления. ООО арендовало часть цеха завода № 22 вместе с универсальным оборудованием для механообработки. Предприятие сформировало портфель заказов на ближайшие 3 месяца, состоящий из фурнитуры и запорных устройств различной конструкции. Численность персонала ООО «КапраЛ» составляла 22 чел., в том числе генеральный директор Филипов А.А., главный инженер, главный бухгалтер, основные и вспомогательные рабочие.

Руководитель этого предприятия Филипов А.А. на одной из выставок встретил изобретателя Анашкина Н.Н, который был готов продать права на свое изобретение – универсальное водоотталкивающее защитное наружное двухфазное покрытие (полимерную масса и аэрозоль-полимеризатор). Данное покрытие предполагает нанесение на разные типы стен. Проникновение влаги сквозь слой покрытия, согласно заключению экспертизы, не превышало 0,1%, что существенно превосходило все существующие аналоги. Анашкин готов был передать полный пакет технической документации за 600 тыс. руб., с возможной отсрочкой выплаты в течение 1 года.

Потенциальными потребителями нового продукта могли бы быть строительные организации, коммунальные службы города, владельцы загородных домов.

Производство компонентов покрытия ориентировано на местное сырье, однако в состав аэрозоли-полимеризатора входит ингредиент, закупаемый в Италии.

Заполнение отчета

Состав подгруппы: Краснова А.А. – руководитель группы, Круть Е.Е. – секретарь группы, Жилин М.М. – эксперт по расчетам, Феоктистова О.О. – эксперт по логике.

1. Оценка значимости мнений экспертов

1) Критерии оценки значимости мнений экспертов и шкалы оценок:

I. Профессиональный опыт в области производства строительных материалов

0 – нет опыта

1 – имеет общее теоретическое представление

2 – имеет опыт в смежных областях деятельности

3 – имеет практический опыт в данной области

II. Общая эрудиция

0 – практически неграмотен

1 – имеет элементарные знания

2 – узкий специалист

3 – эрудит

III. Теоретические знания в области производства строительных материалов

0 – не имеет представления о проблеме

1 – представляет теорию организации производства строительных материалов

2 – поверхностно изучал теорию организации производства строительных материалов

3 – глубоко изучал теорию организации производства строительных материалов

IV. Знание рынка строительных материалов

0 – не имеет представления о рынке строительных материалов,

1 – имеет самое общее представления о рынке строительных материалов

2 – имеет поверхностный опыт работы на рынке строительных материалов

3 – глубоко изучал рынок строительных материалов

2) Оценка значимости критериев компетентности экспертов

Таблица 1.1 – Ранжирование критериев компетентности экспертов

Критерии	I	II	III	IV
Ранги	2	3	4	1

Таблица 1.2 – Расчет рангов критериев (обобщение мнений экспертов)

Эксперт	Критерии				
	I	II	III	IV	
Краснова А.А.	2	3	4	1	
Круть Е.Е.	3	2	4	1	
Жилин М.М.	1	3	3	2	
Феоктистова О.О.	2	4	3	1	
Сумма рангов	2+3+1+2=8	12	15	5	8+12+15+5=40
Вспом. расчет	40:8=5	3,33	2,67	8	5+3,33+2,67+8=19
Вес критерия	5:19=0,26	0,18	0,14	0,42	

3) Оценка весов значимости мнений экспертов

Таблица 1.3 – Оценка компетентности экспертов

Оцениваемые	Критерии			
	I (0,26)	II (0,18)	III (0,14)	IV (0,42)
Краснова А.А.	1	2	1	2
Круть Е.Е.	2	3	1	1
Жилин М.М.	1	3	2	2
Феоктистова О.О.	1	2	2	3

Таблица 1.4 – Сводная таблица расчетов рангов экспертов

Оцениваемые	Критерии				Ранг эксперта	Вес эксп. мнения
	I (0,26)	II (0,18)	III (0,14)	IV (0,42)		
Краснова А.А.	1+2+1+1=5	9	6	8	7,12*)	0,23***)
Круть Е.Е.	10	8	9	11	9,92	0,32
Жилин М.М.	6	7	10	9	8,00	0,27
Феоктистова О.О.	5	5	6	6	5,56	0,18
ИТОГО					30,6**)	1,00

*) 5·0,26+9·0,18+6·0,14+8·0,42=7,12
**)7,12+9,92+8+5,56=30,6
***)7,12:30,6=0,23

2. Возможные риски освоения производства водоотталкивающего покрытия

Таблица 1.5 – Возможные риски

№ п/п	Риск	Код риска
1	невозможность приобретения дополнительного технологического оборудования	(4)
2	сложность освоения технологии изготовления и упаковки компонентов покрытия	(5)
3	высокая себестоимость производства	(6)
4	недостаточно большая емкость рынка	(7)
5	неэффективность рекламы	(8)
6	~~отсутствие квалифицированного персонала~~	
7	экологические проблемы производства аэрозолей	(1)
8	препятствия при выходе на рынок (давление конкурентов и криминал)	(2)
9	недостаточная патентная чистота	(3)
10	проблемы с поставками сырья для полимеризатора	(9)
11	ошибочное позиционирование нового товара	(10)
12	сложность эксплуатации и обслуживания приобретаемого оборудования	(11)
13	проблемы с финансированием освоения производства	(12)
14	появление на рынке аналогичного продукта лучшего качества	(13)
15	конфликты между старым и новым персоналом	(14)
16	противодействие администрации завода	(15)
17	рост курсовой стоимости валюты	(16)

3. Оценка критериев значимости рисков

1) Список критериев важности рисков

(1) Возможность возникновения рисковой ситуации

(2) Увеличение затрат на реализацию проекта освоения производства и реализации водоотталкивающего покрытия

(3) Увеличение сроков реализации проекта освоения производства и реализации водоотталкивающего покрытия

(4) Провал проекта

2) Ранжирование критериев важности рисков

Таблица 1.6 – Ранжирование критериев важности рисков

Критерии	(1)	(2)	(3)	(4)
Ранги	2	3	4	1

3) Расчет рангов и весов критериев важности рисков

Таблица 1.7 – Расчет рангов и весов критериев важности рисков

Эксперт	Ранг	Критерии				
		(1)	(2)	(3)	(4)	
Краснова А.А.	0,23	2	3	4	1	
Круть Е.Е.	0,32	2	4	3	1	
Жилин М.М.	0,27	1	4	3	2	
Феоктистова О.О.	0,18	2	3	4	1	
Ранг		0,23·2+0,32·2+ +0,27·1+0,18·2=1,73	3,59	3,41	1,27	1,73+3,59+ +3,41+1,27=10
Вспом. расчет		10:1,72=5,78	2,79	2,93	7,78	5,78+2,79+ +2,93+7,78=19,38
Вес критерия		5,78:19,38=0,30	0,14	0,15	0,41	

4. Ранжирование рисков по критериям

1) Оценка рисков по критериям (индивидуальное мнение)

Таблица 1.8 – Оценка рисков по критериям (индивидуальное мнение)

Код риска	Сущность риска	Критерии				Ранг
		(1) 0,30	(2) 0,14	(3) 0,15	(4) (0,41)	
(4)	невозможность приобретения дополнительного технологического оборудования	1	11	15	11	1·0,30+11·0,14+ +15·0,15+11·0,41=8,6 (8)
(5)	сложность освоения технологии изготовления и упаковки компонентов покрытия	2	16	16	1	5,65 (3)
(6)	высокая себестоимость производства	5	8	14	10	8,82 (9)

Продолжение табл. 1.8

Код риска	Сущность риска	Критерии				Ранг
		(1) 0,30	(2) 0,14	(3) 0,15	(4) (0,41)	
(7)	недостаточно большая емкость рынка	6	9	13	12	9,93 (12)
(8)	неэффективность рекламы	3	6	12	2	4,36 (1)
(1)	экологические проблемы производства аэрозолей	7	7	1	3	4,46 (2)
(2)	препятствия при выходе на рынок (давление конкурентов и криминал)	4	5	2	9	5,89 (4)
(3)	недостаточная патентная чистота	14	10	11	4	8,89 (11)
(9)	проблемы с поставками сырья для полимеризатора	11	4	8	13	10,39 (13)
(10)	ошибочное позиционирование нового товара	8	15	3	5	7,00 (6)
(11)	сложность эксплуатации и обслуживания приобретаемого оборудования	9	3	4	8	7,00 (5)
(12)	проблемы с освоения производства финансированием	10	13	9	14	11,91 (14)
(13)	появление на рынке аналогичного продукта лучшего качества	12	12	6	16	12,74 (15)
(14)	конфликты между старым и новым персоналом	13	2	10	6	8,14 (7)
(15)	противодействие администрации завода	15	14	5	15	13,36 (16)
(16)	рост курсовой стоимости валюты	16	1	7	7	8,86 (10)

2) Оценка рисков по критериям (коллективное мнение)

Таблица 1.9 – Оценка рисков по критериям (коллективное мнение)

Код риска	Краснова А.А. (0,23)	Круть Е.Е. (0,32)	Жилин М.М. (0,27)	Феоктистова О.О. (0,18)	Расчетный ранг и приоритет
(1)	8	12	1	16	0,23·8+0,32·12+ +0,27·1+0,18·16=8,83 (9)
(2)	3	4	16	1	6,47 (5)
(3)	9	14	2	1	7,27 (6)
(4)	12	1	5	10	6,23 (4)
(5)	1	9	10	15	8,51 (7)

Продолжение табл. 1.9

Код риска	Краснова А.А. (0,23)	Круть Е.Е. (0,32)	Жилин М.М. (0,27)	Феоктистова О.О. (0,18)	Расчетный ранг и приоритет
(6)	2	13	15	2	9,03 (11)
(7)	4	2	3	12	4,53 (1)
(8)	11	10	11	14	11,22 (15)
(9)	13	3	4	3	5,57 (2)
(10)	6	11	12	4	8,86 (10)
(11)	5	5	6	8	5,81 (3)
(12)	14	15	13	5	12,43 (16)
(13)	15	6	7	13	9,60 (12)
(14)	7	16	8	9	10,51 (13)
(15)	16	7	14	6	10,78 (14)
(16)	10	8	9	7	8,55 (8)

5. Составление перечня 10 важнейших рисков

Таблица 1.10 – Десять важнейших рисков

Код риска	Содержание риска
(7)	препятствия при выходе на рынок (давление конкурентов и криминал)
(9)	проблемы с поставками сырья для полимеризатора
(11)	сложность эксплуатации и обслуживания приобретаемого оборудования
(4)	недостаточно большая емкость рынка
(2)	сложность освоения технологии изготовления и упаковки компонентов покрытия
(3)	высокая себестоимость производства
(5)	неэффективность рекламы
(16)	рост курсовой стоимости валюты
(1)	невозможность приобретения дополнительного технологического оборудования
(10)	ошибочное позиционирование нового товара

Практическая работа № 2
ОБОСНОВАНИЕ РИСКОВЫХ РЕШЕНИЙ МЕТОДОМ «ДЕРЕВА РЕШЕНИЙ»

Цель работы – используя метод «дерева решений» научиться рассчитывать вероятность каждого сценария развития проекта, а также ряд других принципиально важных как для анализа рисков проекта, так и для принятия управленческих решений показателей.

Теоретические сведения

Метод "дерева решений". Если имеют место два или более последовательных множества решений, причем последующие решения основываются на результатах предыдущих, и (или) два или более множества состояний среды (т.е. появляется целая цепочка решений, вытекающих одно из другого, которые соответствуют событиям, происходящим с некоторой известной или заданной вероятностью), используется "дерево решений".

С его помощью часто оценивают риск по проектам, при реализации которых инвестирование средств происходит в течение длительного периода времени.

"Дерево решений" – это графическое изображение последовательности решений и состояний окружающей среды с указанием соответствующих вероятностей и выигрышей для любых комбинаций альтернатив и состояний сред (рис. 2.1).

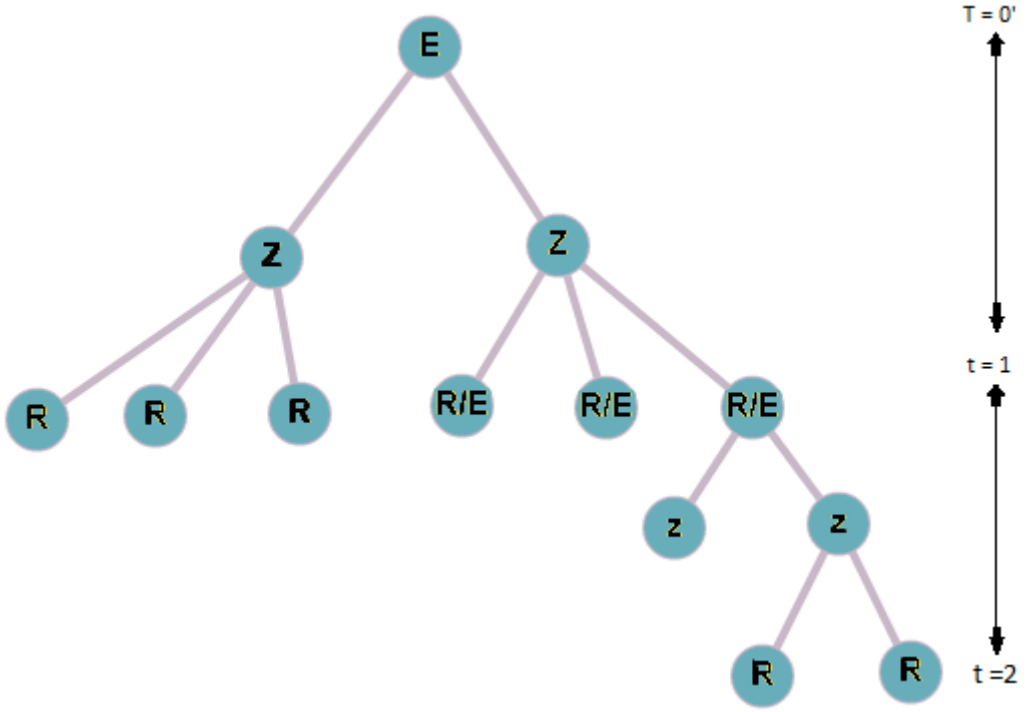


Рис. 2.1. Формальная структура "дерева решений"

Здесь E – узел решения, т.е. узел, характеризующий момент принятия решения; e – линия, представляющая альтернативу решения; Z – узел события, т.е. узел, обозначающий случайное событие; z – линия, описывающая состояние окружающей среды, явившейся следствием наступления случайного события; R – узел результата, т.е. узел, обозначающий результаты, связанные с определенными альтернативными решениями и состояниями окружающей среды; R/E – узел, обозначающий наличие определенного результата и необходимость принятия решения.

Аналитик проекта, осуществляющий построение "дерева решений", для формулирования различных сценариев развития проекта должен обладать необходимой и достоверной информацией с учетом вероятности и времени их наступления.

Можно предложить следующую последовательность сбора данных для построения «дерева решений»:

– определение состава и продолжительности фаз жизненного цикла проекта;

– определение ключевых событий, которые могут повлиять на дальнейшее развитие проекта;

– определение времени наступления ключевых событий;

– формулировка всех возможных решений, которые могут быть приняты в результате наступления каждого ключевого события;

– определение вероятности принятия каждого решения;

– определение стоимости каждого этапа осуществления проекта (стоимости работ между ключевыми событиями) в текущих ценах.

На основании полученных данных строится "дерево решений", структура которого содержит узлы, представляющие собой ключевые события (точки принятия решений), и ветви, соединяющие узлы, – работы по реализации проекта.

В результате построения "дерева решений" рассчитываются вероятность каждого сценария развития проекта, NPV (Net Present Value) – чистая приведенная стоимость, учитывающая временную стоимость денег, см. примечание*) по каждому сценарию, а также ряд других принципиально важных как для анализа рисков проекта, так и для принятия управленческих решений показателей.

Построение "дерева решений" обычно используется для проектов, которые имеют обозримое количество вариантов развития. В противном случае "дерево решений" принимает очень большой объем, так что затрудняется не только вычисление оптимального решения, но и определение данных.

Метод полезен в ситуациях, когда более поздние решения сильно зависят от решений, принятых ранее, но, в свою очередь, определяют дальнейшее развитие событий.

Рассмотрим для наглядности пример использования данного метода.

Пример. Пусть необходимо выбрать лучший из трех возможных инвестиционных проектов: ИП1, ИП2, ИП3. Допустим, что для своего осуществления упомянутые проекты требуют вложения средств в размерах 200, 300 и 500 млн руб. и могут дать прибыль в размере 100, 200 и 300 млн руб. Риск потери средств по этим проектам характеризуется вероятностями на уровне 10, 5 и 20 % соответственно. Какой проект лучше?

Ответить на вопрос чисто математическими средствами трудно. С помощью "дерева решений" этот ответ найти очень просто. «Дерево решений» для условий данного примера представлено на рис. 2.2.

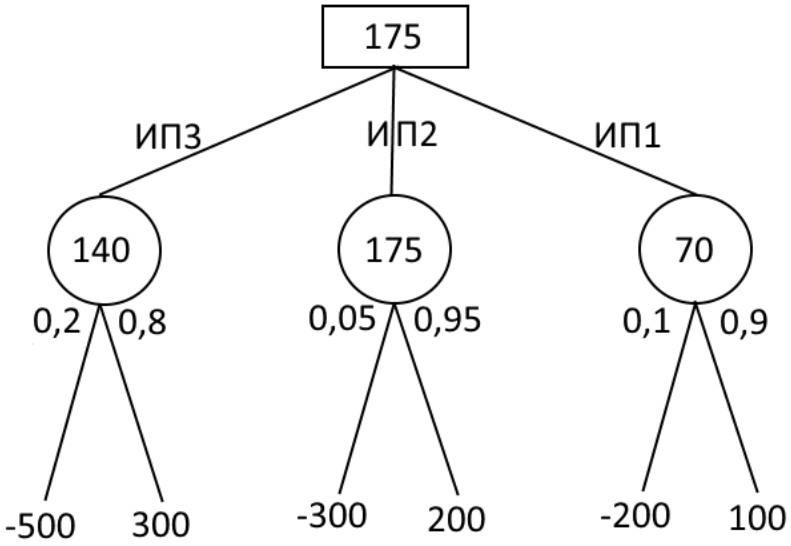


Рис. 2.2. Пример составления "дерева решений"

После составления "дерева решений" начинается его обратный анализ. Идя по "дереву" справа налево и попадая в кружки, мы должны поставить в них математические ожидания выплат. Расчет последних выглядит так:

$$M(x_1) = 100 \cdot 0{,}9 - 200 \cdot 0{,}1 = 70$$
$$M(x_2) = 200 \cdot 0{,}95 - 200 \cdot 0{,}05 = 175$$
$$M(x_3) = 300 \cdot 0{,}8 - 500 \cdot 0{,}2 = 140 \qquad (2.1)$$

Эти математические ожидания и поставлены нами в кружки, изображающие узлы возникновения неопределенностей.

Двигаясь налево, мы попадаем в квадрат и обязаны поставить в него максимальную величину из тех, что стоят на концах, выходящих из него ветвей. В нашем случае оптимальным является решение вложить средства в ИП2.

Порядок обоснования решения

1. Выбор критерия принятия решения – показателя, по максимальному или минимальному значению которого определяется та или иная альтернатива.

Как правило, критерий формулируется на основе одного из принципов:

- минимума потерь (убытков, издержек и др.);
- максимума выигрыша (прибыли, доходов, продаж и т.п.).

2. Разработка альтернатив принимаемых решений.

Решения должны быть взаимоисключающими и включать все возможные варианты: других альтернатив решений существовать не должно.

3. Прогнозирование последствий принимаемых решений (What-If анализ):

- определение логической последовательности событий;
- построение дерева решений (графа);
- проверка, является ли перечень последствий исчерпывающим.

4. Оценка последующих событий:

- вероятность наступления события
- последствия наступления события
- определение параметров дерева решений (характеристик графа)

5. Оценка последствий принимаемых решений по формуле математического ожидания:

$$M_o = \sum_{i=1}^{n} p_i \cdot X_i \qquad (2.2)$$

где M_0 – математическое ожидание результата выбора альтернативы;

p_i – вероятность i-го события;

X_i – последствия наступления i-го события.

6. Выбор альтернативы, являющейся наилучшей по данному критерию (минимум или максимум последствий).

Ситуация-пример для выполнения практической работы

Компания «ГДиК» оказывает посреднические услуги в области материально-технического снабжения крупных российских металлургических предприятий. Часть поставщиков находится в Украине. По причинам политического характера поставки были приостановлены, в результате один из металлургических комбинатов понес убытки в размере 3 млн руб. Руководство комбината обратилось в суд с иском о взыскании ущерба с компании «ГДиК», не обеспечивающей условий договора о поставках материалов. Компания «ГДиК» пригласила украинского адвоката, имеющего возможность доказать, что причины недопоставки носили характер форс-мажорных. Адвокат подписал соглашение об оплате услуг в размере 2000 рублей в час.

Адвокат может прилететь на самолете, добраться на поезде или автомобиле. Стоимость авиабилета (туда и обратно) 25000 рублей, время в пути 2 часа в один конец. Вероятность авиакатастрофы составляет 0,001%.

Стоимость железнодорожного билета (туда и обратно) 10000 рублей, время в пути 30 часов в один конец. Вероятность железнодорожной катастрофы 0,0001 %. Общие расходы на проезд в автомобиле (туда и обратно) составляют 3000 рублей, время в пути 40 часов в один конец. Вероятность автомобильной аварии 0,01 %. Вероятность задержки авиарейса составляет 20%, средняя продолжительность задержки рейсов 6 часов. Вероятность опоздания поезда 30 %, среднее опоздание составляет 3 часа. Вероятность проблем пересечения границы составляет 3 %. Паспортно-таможенный контроль занимает 2 часа. Продолжительность судебного разбирательства 5 часов. Неявка адвоката не является основанием для переноса слушания дела.

Адвокат представлял защиту на 150 судебных разбирательствах, и только 5 процессов были проиграны им.

Без документов, которыми располагает адвокат, вынесение судебного решения в пользу компании «ГДиК» невозможно.

Разбор ситуации

1. Критерий – минимум потерь
2. Альтернативы:
   a. Лететь самолетом
   b. Ехать поездом
   c. Ехать на автомобиле
   d. Без адвоката
3. Последствия (на примере авиаперелета, см. расчет).
4. Заполнение параметров дерева (см. рис. 2.3).
5. Оценка последствий (пример только для авиаперелета, остальные альтернативы студенты выполняют самостоятельно, см. расчет).
6. Выбор: ехать поездом, так как результат обеспечивает минимальные потери по сравнению со всеми другими вариантами.

Чистый приведенный доход, чистая приведенная стоимость, NPV – финансовый метод оценки ИТ-проектов, при котором эффект проекта – это разница между текущими расходами и доходами; показывает, будет у инвестора экономическая прибыль или нет. Отвечает на главный вопрос – насколько поступления будут оправдывать затраты на ИТ, которые мы несем сегодня.

Этот метод основан на сопоставлении величины исходных инвестиций (IC) с общей суммой дисконтированных чистых денежных поступлений, генерируемых в течение прогнозируемого срока. Поскольку приток денежных средств распределен во времени, он дисконтируется с помощью коэффициента r, устанавливаемого аналитиком (инвестором) самостоятельно исходя из ежегодного процента возврата, который он хочет или может иметь на инвестируемый им капитал.

Допустим, делается прогноз, что инвестиции (IC) будут генерировать в течение n лет, годовые доходы в размере P_1, P_2, ..., P_n. Общая накопленная величина дисконтированных доходов (PV) и чистый приведенный эффект (NPV) соответственно рассчитываются по формулам:

$$PV = \sum_k^n \frac{P_k}{(1+r)^k} \tag{2.3}$$

$$NPV = \sum_k^n \frac{P_k}{(1+r)^k} IC \tag{2.4}$$

Очевидно, что если

NPV > 0, то проект принесет прибыль сверх ожидаемой;

NPV < 0, то по проекту ожидается «убыток»;

NPV = 0, то проект соответствует ожиданиям инвестора.

При прогнозировании доходов по годам необходимо по возможности учитывать все виды поступлений как производственного, так и непроизводственного характера, которые могут быть ассоциированы с данным проектом. Так, если по окончании периода реализации проекта планируется поступление средств в виде ликвидационной стоимости оборудования или высвобождения части оборотных средств, они должны быть учтены как доходы соответствующих периодов.

Если проект предполагает не разовую инвестицию, а последовательное инвестирование финансовых ресурсов в течение m лет, то формула для расчета NPV модифицируется следующим образом:

$$NPV = \sum_{k-1}^n \frac{P_k}{(1+r)^k} - \sum_{j-1}^m \frac{IC_j}{(1+i)^j} \tag{2.5}$$

где i – прогнозируемый средний уровень инфляции.

Необходимо отметить, что показатель NPV отражает прогнозную оценку изменения экономического потенциала предприятия в случае принятия рассматриваемого проекта. Этот показатель аддитивен во временном аспекте, т. е. NPV различных проектов можно суммировать. Это очень важное свойство, выделяющее этот критерий из всех остальных и позволяющее использовать его в качестве основного при анализе оптимальности инвестиционного портфеля.

Однако корректное использование NPV-метода возможно только при соблюдении ряда условий.

1. Объем денежных потоков в рамках инвестиционного проекта должен быть оценен для всего планового периода и привязан к определенным временным интервалам.

2. При расчете NPV, как правило, используется постоянная ставка дисконтирования, однако в зависимости от обстоятельств (например, ожидается изменение уровня процентных ставок) ставка дисконтирования может дифференцироваться по годам. Если в ходе расчетов применяются

различные ставки дисконтирования, то, во-первых, данные формулы неприменимы и, во-вторых, проект, приемлемый при постоянной ставке дисконтирования, может стать неприемлемым.

В таблице 2.1 приведен обзор основных методов оценки эффективности внедрения ИТ, указаны их достоинства и недостатки.

Таблица 2.1 – Сравнительный анализ существующих методов оценки эффективности ИТ-проектов

Название метода	Особенности метода	Достоинства	Недостатки
Чистый приведенный доход, NPV	Эффект проекта – это разница между текущими расходами и доходами; показывает, будет у нас экономическая прибыль или нет	Отвечает на главный вопрос – насколько поступления будут оправдывать затраты на ИТ, которые мы несем сегодня	Нет анализа рисков
Индекс рентабельности инвестиций, ROI	Представляет собой общий анализ прибыли инвестиций в активы	Указывает относительное превышение выгоды, которую мы получим, над первоначальными вложениями капитала	Нет анализа рисков
Внутренняя норма доходности, IRR	Позволяет определять процентную ставку от выполнения проекта, а затем необходимо сравнить эту ставку со ставкой окупаемости, учитывая риски	Позволяет сравнивать проекты с абсолютно разным уровнем финансирования	Сложность в расчетах
Срок окупаемости проекта (payback)	Представляет собой период, в течение которого общий эффект возмещает капитал, вложенный на первом этапе	Явно виден, чем будет меньше срок окупаемости, тем проект будет более привлекательным	Не учитывает будущей стоимости денег
Экономическая добавленная стоимость, EVA	В основе его лежит вычисление разницы между чистой операционной прибылью фирмы и всеми затратами, которые может понести фирма на внедрение ИТ	Может применяться для оценки эффективности как отдельного проекта, так и в целом для оценки преобразований ИТ-инфраструктуры	Использовать результаты расчета можно лишь в динамике

Продолжение табл. 2.1

Название метода	Особенности метода	Достоинства	Недостатки
Полная стоимость владения, TCO	Является более эффективной для оценки общей суммы затрат фирмы на ИТ-инфраструктуру, которая включает прямые и косвенные затраты	Дает возможность сравнивать эффективность с другими компаниями аналогичного профиля	Не может быть оценено качество и время разработки новой продукции
Сбалансированная система показателей ИТ, BITS	Наиболее применима для анализа деятельности сервисной ИТ-службы фирмы. По каждому направлению определяются цели, которые характеризуют в будущем желаемое место ИТ в компании	Имеется дополнительная формализация показателей эффективности	Для конкретного предприятия сами показатели, а также их количество может быть разным
Информационная экономика, IE	ИТ-проект оценивают на соответствие разработанным критериям	Определяются приоритеты проектных критериев еще до того, как рассматривается какой-либо ИТ-проект, а также расставляются приоритеты бизнеса предприятия	Субъективизм, который проявляется в анализе рисков проекта
Управление портфелем активов, PM	Предлагается рассматривать инвестиции в ИТ, а также сотрудников ИТ-отделов как активы (а не как затратную часть), которыми управляют по тем же правилам и принципам, как и другими любыми инвестициями	Руководитель ИТ отдела предприятия ведет постоянный контроль над вложениями капитала и оценивает инвестиции по критериям затрат, рисков и выгод, как самостоятельный инвестиционный проект	Переход на использование этого метода влечет за собой как реорганизацию системы управления, так и изменение организационной структуры Компании

Окончание табл. 2.1

Название метода	Особенности метода	Достоинства	Недостатки
Совокупный экономический эффект, TEI	Позволяет оценить проект внедрения любого компонента информационной системы	Возможность анализа рисков	Достаточно узкий спектр применения
Быстрое экономическое обоснование, REJ	Оценивание ИТ с точки зрения бизнес-приоритетов компании, стратегических планов ее развития и основных финансовых показателей	Помогает найти общий язык IT-специалистам и бизнес-менеджменту, а также позволяет оценить вклад IT в бизнес-результат компании	Не может эффективно оценивать проекты преобразования IT-инфраструктуры в целом
Справедливая цена опционов, ROV	ИТ-проект рассматривается с позиции его управляемости в процессе этого проекта	Возможность влиять на оцениваемые параметры по ходу проекта	Весьма трудный и требует много времени для проведения анализа

Примечание: варианты заданий к практической работе № 2 приведены в Приложении Б.

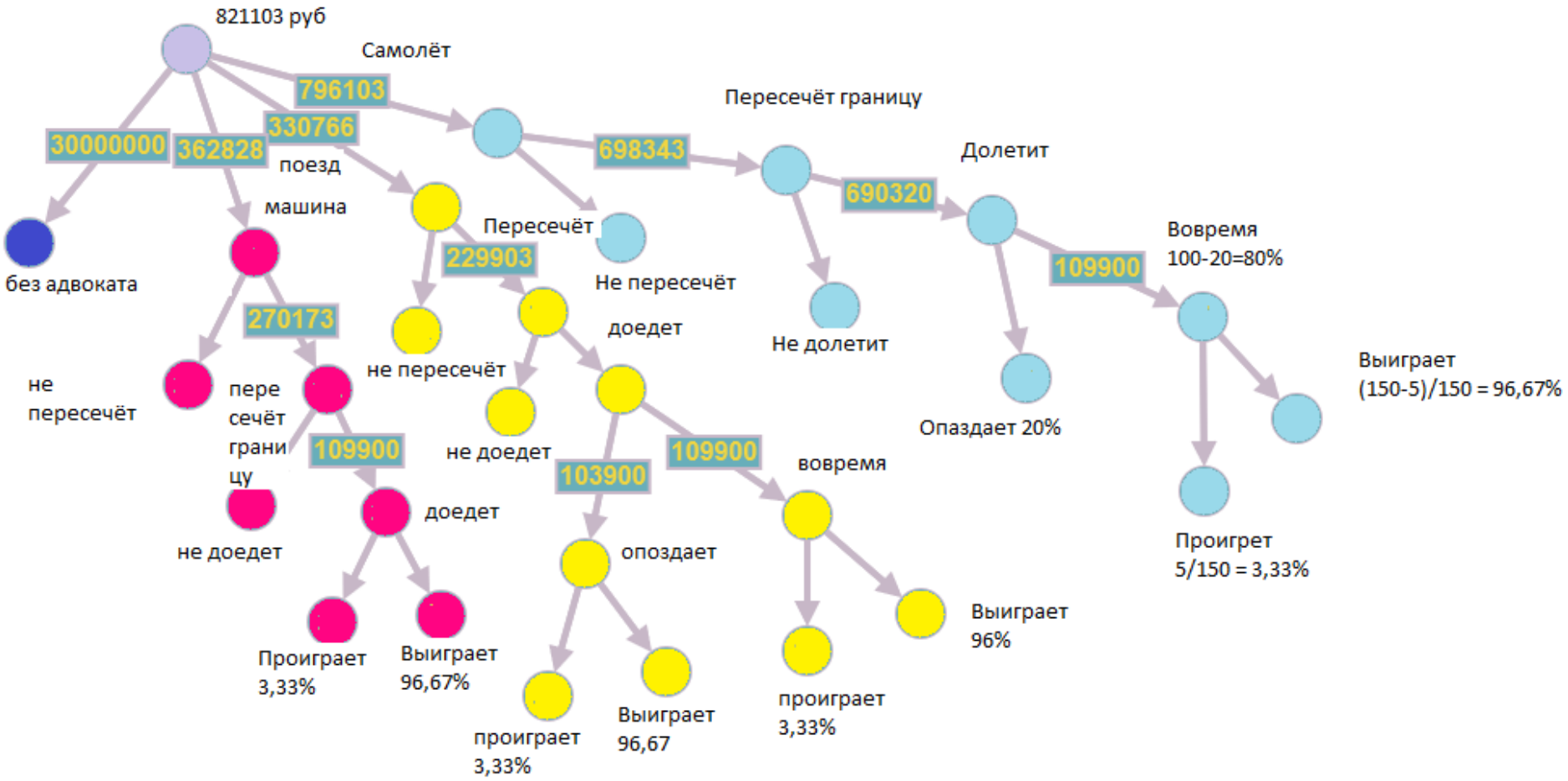


Рис. 2.3. Расчет

Практическая работа № 3
АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ МОДЕЛИ УГРОЗ И УЯЗВИМОСТЕЙ

Цель: изучение базовых принципов построения и приобретение навыков использования модели угроз и уязвимостей ИС при анализе рисков информационной безопасности в корпоративных информационных системах.

Теоретические сведения

Обеспечение безопасности информации носит комплексный характер и основано, среди прочего, на анализе возможных негативных последствий развертывания и эксплуатации ИС.

Модель угроз и уязвимостей предназначена для оценки защищенности ИС, при которой моделирование нарушений безопасности осуществляется на базе анализа цепочки "уязвимость угроза-ресурс". При этом необходимо убедиться, что все ресурсы и уязвимости идентифицированы и сопоставлены с угрозами. Важно иметь возможность при необходимости, не меняя самого методического инструментария, вводить новые виды угроз и уязвимостей, которые станут известны вследствие развития знаний в этой области. В результате анализа по модели угроз и уязвимостей вычисляется уровень риска нарушения безопасности ИС и определяются его возможные причины.

Понятийный базис модели:

− угроза – действие, которое потенциально может привести к нарушению безопасности. Свойством угрозы является перечень уязвимостей, при помощи которых она может быть реализована;

− уязвимость - "слабое" место в ИС, которое может привести к нарушению безопасности путем реализации некоторой угрозы. Свойствами уязвимости являются вероятность (простота) и критичность реализации угрозы через данную уязвимость;

− вероятность реализации угрозы через данную уязвимость в течение года – степень возможности реализации угрозы через данную уязвимость в тех или иных условиях. Измеряется в процентах;

− критичность реализации угрозы – степень влияния реализации угрозы на ресурс, т. е. как сильно реализация угрозы повлияет на работу ресурса. Задается в процентах. Допустимо рассматривать критичность реализации угрозы и по составляющим безопасности (конфиденциальности, целостности и доступности), и в целом (с учетом всех трех рисков);

− ресурс – часть ИС, предназначенная для хранения информации, подверженной угрозам ИБ (сервер, рабочая станция, мобильный компьютер, устройство хранения резервных копий и т. д.). Свойствами ресурса в данной модели являются перечень угроз, воздействующих на него, и критичность ресурса;

− критичность ресурса – степень значимости ресурса для ИС, т. е. насколько сильно реализация угроз безопасности на ресурс повлияет на

работу всей ИС. Критичность ресурса оценивают в денежных единицах, относительных уровнях, условных единицах. Чаще всего она оценивается в процентах, т. е. в уровнях от 1 до 100 по отношению к критичности других ресурсов. Критичность можно рассматривать как отдельно по конфиденциальности, целостности и доступности, так и в целом с учетом всех трех рисков;

– максимальное критичное время простоя – значение времени простоя, которое является критичным для компании. Ущерб, нанесенный компании при простом ресурсе в течение этого времени, достигает максимального значения. При дальнейшем простое ущерб, наносимый компании, уже не увеличивается. Эта характеристика используется для оценки критичности ресурса по угрозе доступности.

Критичность ресурса оценивается, как правило, из ущерба, который понесет компания при осуществлении угроз нарушения конфиденциальности, доступности или целостности. При рассмотрении этой характеристики необходимо определить шкалу, используемую для классификации критичности.

Для каждого из ресурсов определяются список угроз, действующих на него, и список уязвимостей. Для нарушения безопасности по одной угрозе нарушитель может воспользоваться разными уязвимостями. Одна и та же уязвимость может привести к нарушению безопасности по нескольким угрозам (рис. 3.1).

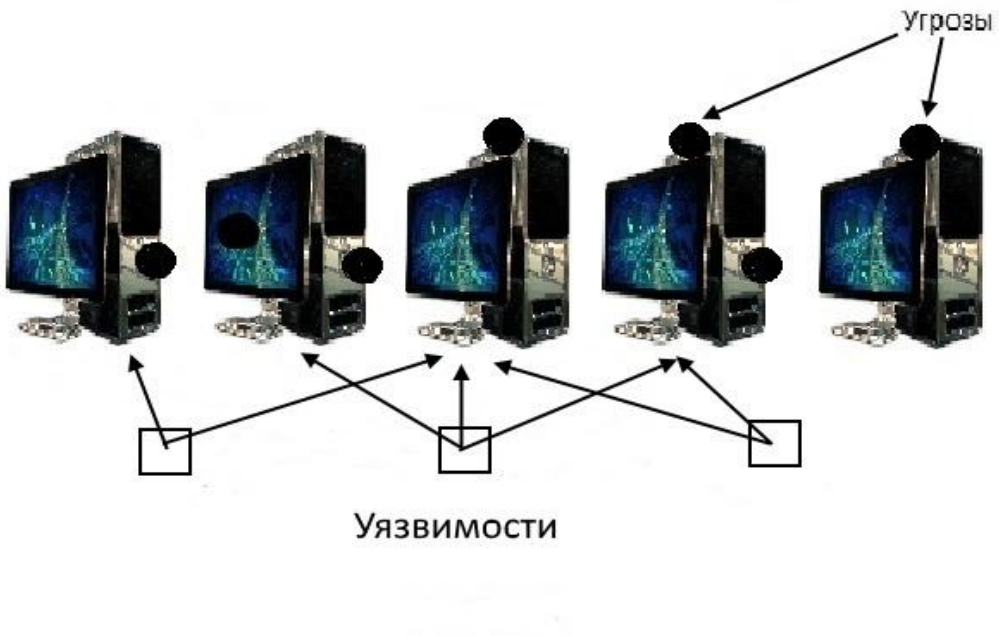


Рис. 3.1. Связь угроз и уязвимостей

Количественное значение риска рассчитывают с помощью функций:

$R_{угр,уяз}(P_{уяз}, K_{уяз})$ – риск от реализации угрозы через уязвимость, где $P_{уяз}$ – вероятность реализации угрозы через уязвимость; $K_{уяз}$ – критичность реализации угрозы через уязвимость *i*;

$R_{угр}(R_{угр,уяз1}, R_{угр,уяз2}, \dots, R_{угр,уязN})$ – риск от реализации угрозы, где $R_{угр,уязi}$ – риск от реализации угрозы через уязвимость;

$R_{рес}(K_{рес}, R_{угр1}, R_{угр2}, \dots, R_{угрN})$– риск нарушения безопасности ресурса, где $K_{рес}$– критичность ресурса; $R_{угрi}$– риск от реализации угрозыi.

Очевидно, что наличие больших значений вероятностей и критичностей реализации угроз через уязвимости приводит к большому значению. Поэтому задача анализа системы по модели угроз и уязвимостей – поиск, выделение и устранение наиболее критичных и опасных уязвимостей, которым подвержена ИС.

Рассмотренная методика оценки рисков положена в основу отечественного программного комплекса ГРИФ.

Контрольные вопросы

1. Какие компоненты ИС рассматриваются в модели угроз и уязвимостей?
2. Как соотносятся угрозы информационной безопасности и уязвимости ресурсов?
3. В чем отличие критичности реализации угрозы от критичности ресурса?
4. Укажите способы определения угроз нарушения безопасности, которым подвержен ресурс ИС.
5. Предложите формулы для расчета риска нарушения безопасности ресурса ИС.

Порядок выполнения работы

1. Получить у преподавателя описание ИС (Приложение В).
2. Для данной ИС построить модель угроз и уязвимостей:
   - выделить угрозы, применимые к рассматриваемой ИС;
   - выделить уязвимости, через которые могут быть реализованы угрозы;
   - определить угрозы, которые могут воздействовать на каждый из ресурсов в рамках ИС, и обосновать причины наличия этих угроз;
   - определить уязвимости, через которые могут быть реализованы указанные угрозы.
3. Определить вероятности и критичности реализации угроз через уязвимости для каждой пары "угроза-уязвимость".
4. Определить функции для расчета рисков.
5. Рассчитать риски для всех ресурсов в рассматриваемой модели ИС.
6. Провести анализ полученных результатов. Выделить наиболее опасные уязвимости и предложить способы снижения вероятности и критичности. Предложить дальнейший план развития политики информационной безопасности для рассматриваемой ИС.

Содержание отчета

1. Формулировка задачи.
2. Описание построенной модели угроз и уязвимостей.
3. Экспертные оценки вероятности и критичности реализации угроз через уязвимости.
4. Формулы для расчета рисков.
5. Результаты расчета численных значений рисков.
6. Ответы на контрольные вопросы.
7. Выводы по работе.

Пример отчета

Рассмотрим информационный ресурс, представленный рабочей станцией пользователя ИС.

Особенность исследуемой ИС - в ней используется система регулярного резервирования информации и установлено антивирусное ПО. Все, что не указано явно, отсутствует.

Рассмотрим наиболее актуальные угрозы, действующие на рассматриваемый ресурс.

1. Физическое воздействие нарушителя:

− неавторизованное проникновение нарушителя внутрь охраняемого периметра;

− кража носителя информации (бумажного носителя, компакт-дисков, флэш-карты и т.п.).

2. Физическая внешняя угроза: удар молнии.

3. Программные угрозы: исполнение файла, содержащего компьютерный вирус.

Угрозы могут быть реализованы через следующие уязвимости:

− в компании отсутствует регламент доступа н помещения с ценными ресурсами;

− в компании отсутствует система наблюдения за объектом, или существующая система наблюдения охватывает не вес важные объекты;

− отсутствует система резервирования;

− не используется автоматическая зашита электрооборудования;

− не установлено антивирусное программное обеспечение;

− не производится регулярное обновление антивирусного программного обеспечения;

− допущены типовые ошибки при конфигурировании операционной системы.

Определим перечень угроз, которые могут воздействовать на рассматриваемый ресурс.

Угрозы "Неавторизованное проникновение нарушителя внутрь охраняемого периметра", "Удар молнии" и "Запуск зараженных файлов,

которые воздействуют на операционную систему" могут быть направлены на ресурс, так как это не противоречит исходным данным.

Угроза "Кража носителей" не может быть направлена на данный ресурс, гак как он сам не является носителем информации.

Рассмотрим связи уязвимостей с угрозами. Угроза "Неавторизованное проникновение нарушителя внутрь охраняемого периметра" может быть реализована через уязвимости "Отсутствие регламента доступа в помещения с ценными ресурсами", "Отсутствие системы наблюдения (видеонаблюдение, сенсоры и т.д.) за объектом (или существующая система наблюдения охватывает не все важные объекты)". Угроза "Удар молнии" может быть реализована через уязвимости "Отсутствие систем резервирования" и "Не используется автоматическая защита электрооборудования". Система резервирования присутствует в ИС, поэтому этой уязвимости на ресурсе нет. Угроза "Запуск зараженных файлов, которые воздействуют на операционную систему" может быть реализована через уязвимости "Не установлено антивирусное программное обеспечение", "Не производится регулярное обновление антивирусного программного обеспечении", "Допущены типовые ошибки при конфигурировании операционной системы". Поскольку антивирусное программное обеспечение в ИС установлено, то первых двух уязвимостей на ресурсе нет.

Рассмотрим пример расчета рисков для угроз безопасности ИС для одного из ресурсов. Определим для каждой пары "угроза-уязвимость" вероятность и критичность реализации угрозы методом экспертных оценок и построим таблицу соответствия угроз и уязвимостей (например, табл. 3.1).

Таблица 3.1 – Пример оценки критичности реализации угроз

Угроза	Уязвимость	Вероятность реализации угрозы в течение года, %	Критичность реализации угрозы, %
Неавторизованное проникновение нарушителя внутрь охраняемого периметра	Отсутствие регламента доступа в помещения с ценными ресурсами	50	60
	Отсутствие системы наблюдения (видеонаблюдение, сенсоры и т.д.) за объектом (или существующая система наблюдения охватывает не все важные объекты)	20	60

Воспользуемся следующими формулами для расчета рисков нарушения безопасности:

1. Риск реализации угрозы *i* через уязвимость *j*:

$$R_{i,j}\left(P_{i,j}, K_{i,j}\right) = \frac{P}{100}\frac{K}{100} \quad (3.1)$$

2. Риск реализации угрозы *i* по всем уязвимостям:

$$R_i\left(R_{i,j}\right) = 1 - \prod_{j=1}^{n}(1 - R_{i,j}), \quad (3.2)$$

где *n* – количество уязвимостей, через которые может быть реализована угроза.

3. Риск нарушения безопасности ресурса по всем уязвимостям:

$$R(K, R_i) = K(1 - \prod_{i=1}^{m}(1 - R_i)), \quad (3.3)$$

где *m* – количество угроз; *K* – критичность ресурса.

Используя приведенные формулы, рассчитаем риск реализации угроз через уязвимости и определим риск реализации каждой угрозы (табл. 3.2).

Таблица 3.2 – Риски реализации угроз через уязвимости

Угроза	Уязвимость	$R_{i,j}$	R_i
Неавторизованное проникновение нарушителя внутрь охраняемого периметра	Отсутствие регламента доступа в помещения с ценными ресурсами	0,3	0,384
	Отсутствие системы наблюдения (видеонаблюдение, сенсоры и т.д.) за объектом (или существующая система наблюдения охватывает не все важные объекты)	0,12	

Риск нарушений безопасности по ресурсу рассчитывается по всем видам угроз и уязвимостей (расчет здесь не приводится).

Проанализировав ситуацию в целом, можно сделать заключение, что рассмотренный ресурс в значительной мере подвержен рискам нарушений.

Для снижения риска необходимо снижать вероятности реализации угрозы и критичности ее для ресурса. По формуле риск является произведением вероятности на критичность, поэтому необходимо снижать риски для таких пар "угроза – уязвимость", где это произведение максимально (меры по снижению риска здесь не приводятся).

Практическая работа № 4
РАСЧЕТ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПО МЕТОДИКЕ RISKWATCH

Цель работы – изучение расчета рисков информационной безопасности с использованием методики RiskWatch анализа и управления рисками информационной безопасности и приобретение практических навыков расчета.

Теоретические сведения

Анализ рисков, прежде всего, представляет собой комплексную оценку безопасности ИС, конечный результат которой – получение количественных или качественных показателей. Проведение всего комплекса работ по анализу рисков, а затем и по управлению ими вручную является чрезвычайно ресурсозатратным мероприятием, поэтому весь набор действий обычно формализуют и представляют в виде единой методики анализа рисков, которую можно автоматизировать.

Программное обеспечение RiskWatch – пример такой автоматизации. Оно представляет собой мощное средство, ориентированное на точную количественную оценку соотношения потерь от реализации угроз безопасности и затрат на создание системы зашиты. В этом продукте риски в сфере информационной и физической безопасности компьютерной сети предприятия рассматриваются совместно.

В семейство RiskWatch входят программные продукты оценки физических методов защиты, информационных рисков, выполнения требований по ГОСТ 17799.

В качестве критериев для оценки и управления рисками используются показатели:

- ожидаемые годовые потери (annual loss expectancy, ALE);
- оценка возврата инвестиций (return on investment, ROI).

Методика анализа рисков RiskWatch включает четыре этапа.

I. Определение предмета исследования. Здесь описываются тип организации, состав исследуемой ИС. базовые требования в области безопасности, категории защищаемых ресурсов. Для облегчения работы аналитика в шаблонах, соответствующих типу организации, заданы списки категорий защищаемых ресурсов, потерь, угроз, уязвимостей и мер зашиты.

II. Ввод данных, описывающих характеристики ИС. На этом этапе подробно описываются ресурсы, потери и классы инцидентов. Классы инцидентов получаются путем сопоставления категории потерь и категории ресурсов. Для выявления возможных уязвимостей используется анкета-вопросник. Вопросы связаны с категориями ресурсов. Задаются частота возникновения каждой из выделенных угроз, степень уязвимости и ценность

ресурсов. Все это используется в дальнейшем для расчета эффекта от внедрения средств защиты.

III. Количественная оценка. На этом этапе рассчитывается профиль рисков и выбираются меры обеспечения безопасности ИС. Сначала устанавливаются связи между ресурсами, потерями, угрозами и уязвимостями, выделенными на предыдущих этапах.

Риск оценивается с помощью математического ожидания потерь за год. Для расчета оценки ожидаемых годовых потерь *ALE*(в денежных единицах) используется одна из формул:

$$\mathrm{ALE} = \mathrm{AV} \cdot \mathrm{EF} \cdot \mathrm{ARO}, \tag{4.1}$$

где AV (AssetValue) – стоимость актива (данных, программ, аппаратуры и т.д.); EF (ExposureFactor) – коэффициент воздействия (показывает, какая часть (в процентах) от стоимости актива подвергается риску); ARO (AnnualizedRateofOccurrence) – показатель ожидаемой годовой частоты происшествия, т. е. интенсивность нежелательного события (демонстрирует, насколько вероятна реализация определенной угрозы за указанный период времени).

В результате получается оценка ожидаемых годовых потерь для одного конкретного актива от реализации одной угрозы. Когда все активы и воздействия идентифицированы и собраны вместе, то появляется возможность оценить общий риск для всей ИС как сумму всех частных значений ALE.

$$\mathrm{ALE} = \mathrm{ARO} \cdot \mathrm{SLE}, \tag{4.2}$$

где SLE (SingleLossExpectancy) (в денежных единицах) – показатель ожидаемого единичного ущерба.

SLEможет быть рассчитан одним из способов:

– как разница первоначальной стоимости актива и его остаточной стоимости после происшествия;

– как произведение стоимости актива на фактор воздействия:

$$\mathrm{ALE} = \mathrm{AV} \cdot \mathrm{EF}, \tag{4.3}$$

(в этом случае вторая формула расчета ALE идентична первой).

Дополнительно рассматриваются сценарии типа "что если...", которые позволяют описать аналогичные ситуации при условии внедрения средств защиты. Сравнивая ожидаемые потери при условии внедрения защитных мер и без них можно оценить эффект от таких мероприятий. Управление рисками считается эффективным, если расход на безопасность в год не превышают ожидаемый годовой ущерб.

Эффект от внедрения средств защиты количественно описывается с помощью показателя отдачи от инвестиций ROI:

$$ROI = \sum_{(i)} NPV(Benefits_i) - \sum_{(i)} NPV(Costs_i), \quad (4.4)$$

где $Costs_i$ – затраты (в денежных единицах) на внедрение и поддержание меры защиты i; $Benefits_i$, - оценка (в денежных единицах) пользы (т. е. ожидаемого снижения потерь), которую приносит внедрение меры защиты i; NPV (NetPresentValue) – поправка, учитывающая инфляцию.

IV. Генерация отчетов.

Типы отчетов:

– отчет о стоимости защищаемых ресурсов и ожидаемых потерь от реализации угроз;

– отчет об угрозах и мерах противодействия;

– отчет о результатах аудита безопасности.

Рассматриваемая методика позволяет оценить не только те риски, которые сейчас существуют у предприятия, но и ту выгоду, которую может принести внедрение физических, технических, программных и прочих средств и механизмов защиты.

Недостатки методики RiskWatch:

– анализ рисков проводится на программно-техническом уровне защиты без учета организационных и административных факторов;

– полученные оценки рисков не исчерпывают понимание риска с системных позиций, т. с. расчетный метод не учитывает комплексный подход к информационной безопасности;

– программное обеспечение RiskWatch существует только на английском языке и характеризуется высокой стоимостью лицензии.

Методику RiskWatch и средства, поддерживающие ее, выбирают, учитывая:

– наличие экспертов, способных дать точные и достоверные оценки объема потерь от угроз информационной безопасности;

– наличие в компании статистики по инцидентам в сфере информационной безопасности;

– необходимость в точной количественной оценке последствий реализации угроз или достаточность оценки на качественном уровне.

В работе рассматривается математический аппарат, составляющий расчетную основу методики RiskWatch.

Контрольные вопросы

1. Дайте определение качественной оценки риска. В чем заключается ее отличие от количественной оценки?
2. На каких этапах методики RiskWatch производится категоризация ресурсов?
3. Что характеризует показатель SLE? Как он рассчитывается?

4. Перечислите основные факторы, определяющие выбор методики RiskWatch.

5. Какие недостатки присущи методике RiskWatch?

Порядок выполнения работы

1. Получить у преподавателя вариант задания (Приложение Г).
2. Определить показатель ARO.
3. Вычислить показатель SLE (на основании предложенного варианта задания формулу для вычисления SLE определить самостоятельно).
4. Рассчитать оценку годовых потерь ALE.
5. Вычислить эффект от внедрения средств защиты ROI.

Содержание отчета

1. Формулировка задачи.
2. Данные о параметрах заданной области исследования.
3. Формула для вычисления показателя SLE и обоснование выбора данной формулы.
4. Результаты вычислений показателей ARO и ROI.
5. Ответы на контрольные вопросы.
6. Выводы по работе.

Пример отчета

Рассмотрим ситуацию, когда в компании при приобретении новых серверов одноранговая сеть (P2P) заменена на клиент-серверную технологию. В компании работает 200 сотрудников, трудозатраты каждого из них в среднем равны 20 у.е./ч. Ранее на компьютеры компании не было установлено антивирусное программное обеспечение, потому что риск заражения вирусами был минимален. Один из новых серверов предоставляет доступ в Интернет, которым могут воспользоваться все пользователи.

Данные изменения в ИС приводят к повышению уровня вирусного заражения на 80 % (согласно экспертной оценке). На полное восстановление ИС в среднем необходимо потратить 3 часа. Организация решила закупить антивирусное программное обеспечение для защиты всех серверов и компьютеров на общую сумму 4700 у.е. Рассчитаем ожидаемые годовые потери организации и эффект от внедрения защитных мер.

Формальное описание заданной области исследования.

C (Count) – количество сотрудников в организации, *C* = 200.

L (LaborCost) – трудозатраты одного сотрудника в час, *L*= 20.

Cost – сумма, затраченная на покупку антивирусов, *Cost*= 4700.

T(Time) – время, затрачиваемое на восстановление ИС, *T* = 3.

ARO = 0,8. Вероятность вирусной опасности равна 80 %, что в данной области можно рассматривать как показатель ожидаемой частоты происшествия.

Вычислим показатель *SLE*. В данной области можно выделить следующую формулу для расчета *SLE*:

$$\mathrm{SLE} = \mathrm{C} \cdot \mathrm{L} \cdot \mathrm{T} = 200 \cdot 20 \cdot 3 = 1200\,\mathrm{y.e.} \quad (4.5)$$

Тогда оценка годовых потерь

$$ALE = SLE \cdot ARO = 12000 \cdot 0{,}8 = 9600\,y.e. \quad (4.6)$$

Эффект от внедрения средств зашиты *ROI*можно вычислить по формуле

$$ROI = ALE - Cost = 9600 - 4700 = 4900\,y.e. \quad (4.7)$$

Таким образом, компании удастся сохранить 4900 у.е./год при внедрении средств защиты в ИС.

Практическая работа № 5
МЕТОДИКА АНАЛИЗА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ CORAS

Цель работы – изучение методики анализа рисков информационной безопасности CORAS, получение навыков ее практического применения при управлении информационной безопасностью в современных ИС.

Теоретические сведения

Методика CORAS представляет собой комбинацию механизмов описания ИС (язык моделирования UML, моделирование процессов) и разновидностей анализа (Fault Tree Analysis, Effect Criticality Analysis, Markov Analysis и пр.). При разработке методики использованы положения австрало-новозеландского стандарта AS/NZS 4360:1999 "Risk Management" и международного стандарта ISO 17799 "Code of Practice for Information Security Management" (ГОСТРИСО/МЭК 17799). Также были учтены рекомендации, изложенные в документах ISO/IEC TR 13335-1 "Guidelines for the Management of IT Security" и IEC 61508:2000 "Functional Safety of Electrical /Electronic /Programmable Safety Related". В соответствии с положениями методики CORAS, ИС рассматривается не с точки зрения технологий, а с различных сторон как сложный комплекс, даже с учетом влияния человеческого фактора.

Анализ рисков, согласно методике CORAS, состоит из семи фаз.

Фаза 1. Вводный этап - ознакомительный. Основная цель – определение задач, терминологии, защищаемых ресурсов и области анализа. Данная информация собирается аналитиками на основе представлений клиента и обсуждений с ним данных об ИС.

Фаза 2. Анализ высокого уровня – данный этап представляет собой первый анализ угроз, в процессе которого определяются уязвимости и сценарии реализации угроз. Поставленной задачей есть - идентификация ресурсов и основных рисков. Поиск защищаемых ресурсов начинается на данном этапе и продолжается на следующем. Дальнейшая работа ведется относительно этих ресурсов. Результат анализа высокого уровня помогает аналитикам идентифицировать целевые аспекты, упрощая определение области всего анализа. Формализуется информация, полученная от клиента на первом этапе, а также документация в виде UML-диаграмм. Также создается UML-диаграмма пользования ИС. Затем строится первоначальная диаграмма ресурсов, показывающая компоненты ИС и основные ресурсы. Ресурсы подразделяют на прямые и косвенные. Прямые ресурсы могут быть повреждены непосредственно при реализации угрозы. Стрелками показывают взаимосвязи между ресурсами. После установления ресурсов находятся наиболее значимые угрозы и уязвимости, которые заносятся в таблицу высокоуровневых рисков (табл. 5.1).

Таблица 5.1 − Таблица высокоуровневых рисков

Инициатор	Нарушение (способ реализации, состав, объект)	Причина нарушения
...	...	...

Фаза 3. Одобрение - это последний из подготовительных этапов. Основная цель – завершение составления документации, описания цели и ресурсов, а также формальное одобрение клиентом собранной информации. Также определяются шкалы последствии (для нежелательных инцидентов) и шкалы вероятностей. В конце определяются критерии опенки рисков. Ресурсы сортируются в соответствии с их важностью (1 – очень важный, 5 – маловажный), и заполняется таблица ресурсов (табл. 5.2).

Таблица 5.2 − Таблица ресурсов ($R_1, \ldots, R_4$ — ресурсы)

Ресурс	Важность	Тип
R_1	2	Прямой
R_2	3	Прямой
R_3	3	Косвенный
R_4	1	Косвенный

Вероятностные шкалы инцидентов и ущерб, который они приносят ресурсам, определяются по следующему правилу: самая низкая вероятность инцидента –«редко»– устанавливается при одном случае инцидента на всем жизненном цикле ИС; остальные интервалы имеют увеличивающееся количество ожидаемых событий до достижения максимально возможного количества событий за год. Поскольку инциденты могут оказывать разное влияние в зависимости от поврежденного ресурса, создаются отдельные шкалы последствий для каждого прямого ресурса. В таблицах 5.3 и 5.4 показаны шкала последствий для одного ресурса и вероятностная шкала, определенная для ИС.

Таблица 5.3 − Шкала последствий для одного ресурса

Значимость последствия	Описание
Катастрофическое	Повреждены более 1000 единиц ресурса
Большое	Повреждены 100-1000 единиц ресурса
Умеренное	Повреждены 10-100 единиц ресурса
Небольшое	Повреждены 1-10 единиц ресурса
Незначительное	Нет поврежденных единиц ресурса

Критерии оценки рисков позволяют указать, допустим ли риск для ресурса или необходимо определить и оценить возможные методы борьбы с ним. Эти критерии определяются на основе матрицы оценки рисков по каждому ресурсу. Риск с определенной вероятностью и последствием будет находиться в определенной ячейке матрицы.

Таблица 5.4 − Вероятностная шкала

Значение вероятности	Описание
Несомненно	5 раз или больше в год
Вероятно	2-5 раз в гол
Возможно	1 раз в год
Маловероятно	Меньше 1 раза в год
Редко	Меньше 1 раза в 10 лет

На основе дискуссий клиента и аналитиков принимается решение, как отметить ячейку матрицы: допустимый риск или он должен быть оценен. Матрица оценки рисков представлена в табл. 5.5 (для случая, когда принято решение, используется матрица для всех ресурсов).

Таблица 5.5 − Матрица оценки рисков (риск Д - допустимый, О - должен быть оценен)

Значение вероятности	Значимость последствия				
	Незначительное	Небольшое	Умеренное	Большое	Катастрофическое
Редко	Д	Д	Д	Д	О
Маловероятно	Д	Д	Д	О	О
Возможно	Д	Д	О	О	О
Вероятно	Д	О	О	О	О
Несомненно	О	О	О	О	О

Фаза 4. Идентификация рисков – предназначен для определения рисков, используется структурный подход – проход через всю структуру цели. Цель — выявление как можно большего количества потенциально нежелательных инцидентов, а также уязвимостей, угроз и их сценариев. Идентифицированные риски документируются при помощи языка моделирования рисков. Первоначальные диаграммы сценариев угроз подготавливаются на основе высокоуровневого анализа (см. табл. 5.1). Строятся три диаграммы в соответствии стремя типами угроз: случайные действия, умышленные действия и угрозы, не связанные с человеческим фактором (например, отказ системы).

Фаза 5. Оценка рисков - данный этап направлен на оценку последствий и вероятностных значений по каждому из выявленных нарушений. Значения используются для вычисления значения риска. Оценки вероятности для каждого сценария угрозы добавляются в диаграмму угроз с помощью аннотаций. Если вероятность сценария сложно определить, то аналитик высказывает предположение, основываясь на истории (например, статистика инцидентов безопасности, личный опыт). Вероятности сценариев угроз используются для получения комбинированной вероятности для нежелательных инцидентов. Последствия оцениваются для каждой связи "нежелательный инцидент - ресурс". Значение последствия берется из табл.5.3.

Фаза 6. Вычисление рисков – данный этап состоит из двух частей.

Значение риска определяется с помощью матрицы оценки рисков. В табл. 5.6 показаны риски, расположенные в матрице оценки рисков. Только *P*, находится в пределах допустимого уровня рисков, остальные требуют дальнейшей оценки.

Таблица 5.6 − Матрица оценки рисков ($P_1, \ldots, P_5$ – риски)

Значение частоты	Значимость последствия				
	Незначительное	Небольшое	Умеренное	Большое	Катастрофическое
Редко			P_1		
Маловероятно					P_5
Возможно			$P_{2,3}$		
Вероятно				P_4	
Несомненно					

Фаза 7. Методы противодействия рискам - последний этап направлен на поиск путей устранения рисков, а также на уменьшение затрат. В ходе работ оцениваются неприемлемые риски, чтобы найти способы их уменьшения. Методы противодействия рискам должны способствовать уменьшению вероятностей и последствий инцидентов. Эти методы оцениваются также сточки зрения цены/выгоды перед тем, как будет составлен окончательный план работ. Строятся диаграммы устранения рисков. Первоначальная диаграмма симметрична окончательной диаграмме угроз за исключением того, что каждая связь между нежелательным инцидентом и ресурсом, представляющая неприемлемый риск, обозначена значком риска и идентификатором.

Методика CORAS не предусматривает такой эффективной меры по управлению рисками, как периодичность проведения оценки рисков и обновление их величин, что свидетельствует о том, что методология пригодна для выполнения разовых оценок и трудозатрат на при регулярном применении, но несмотря на то, что в методику CORAS заложена возможность разработки рекомендаций для выбора тех или иных мер по снижению рисков, она не позволяет оценить эффективность инвестиций, вложенных во внедрение мер безопасности. Так же в CORAS не предусмотрены механизмы оценки эффективности способов управления и отсутствует формализованная процедура принятия остаточных рисков.

Плюсами CORAS является то, что программный продукт, реализующий эту методологию, распространяется бесплатно и не требует значительных ресурсов для установки и применения.

Средства программной реализации методики CORAS предоставляют инструменты, направленные на поддержку описания ИС, документирования, сохранения и представления результатов анализа рисков. Приложение

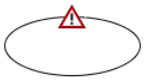
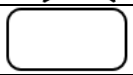
CORAS Tool представляет собой инструмент для описания и оценки рисков. Программа содержит два основных репозитория:

Experience Library – хранилище результатов, которое содержит многоразовые результаты предыдущих анализов в виде UML-модели, контрольные процедуры и многое другое;

Risk Analysis Project– хранилище результатов фактического анализа безопасности.

Для описания различных процессов используется специальный язык CORAS, конструкции которого графически представляются в виде UML-диаграмм, описывающих ИС, промежуточные результаты, а также общие выводы (табл. 5.7).

Таблица 5.7 – Элементы программы (основные элементы UML-диаграмм)

Вид	Название на английском языке	Название на русском языке
	Asset	Ценность, информация, подлежащая защите
	Stakeholder	Владелец информации (заинтересованная сторона)
	Threat Human Accidental	Угроза непреднамеренная, человеческого происхождения
	Threat Human Deliberate	Угроза преднамеренная, человеческого происхождения
	Threat Non Human	Угроза нечеловеческого происхождения
	Threat Scenario	Сценарий угрозы
	Vulnerability	Уязвимость
	Unwanted Incident	Непредсказуемый инцидент
	Risk	Риск
	Treatment	Сценарий устранения(лечения)
	And	И
	Or	ИЛИ
	Region	Регион

Элементы могут быть связаны в виде UML-диаграмм ценностей (рис. 5.1), угроз (рис. 5.2), рисков (рис. 5.3), устранения рисков (рис. 5.4).

Результатом работы программного пакета является отчет, где подробно описаны все диаграммы процессов, рисков, а также выходные данные анализа.

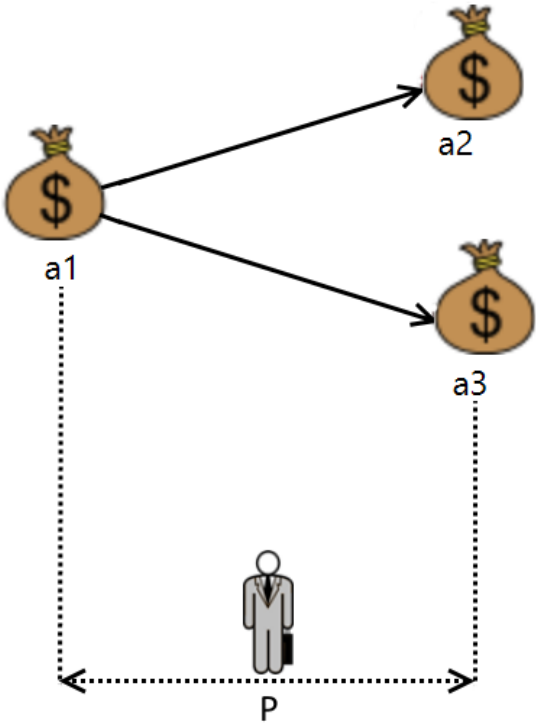


Рис. 5.1. Вид диаграммы ценностей

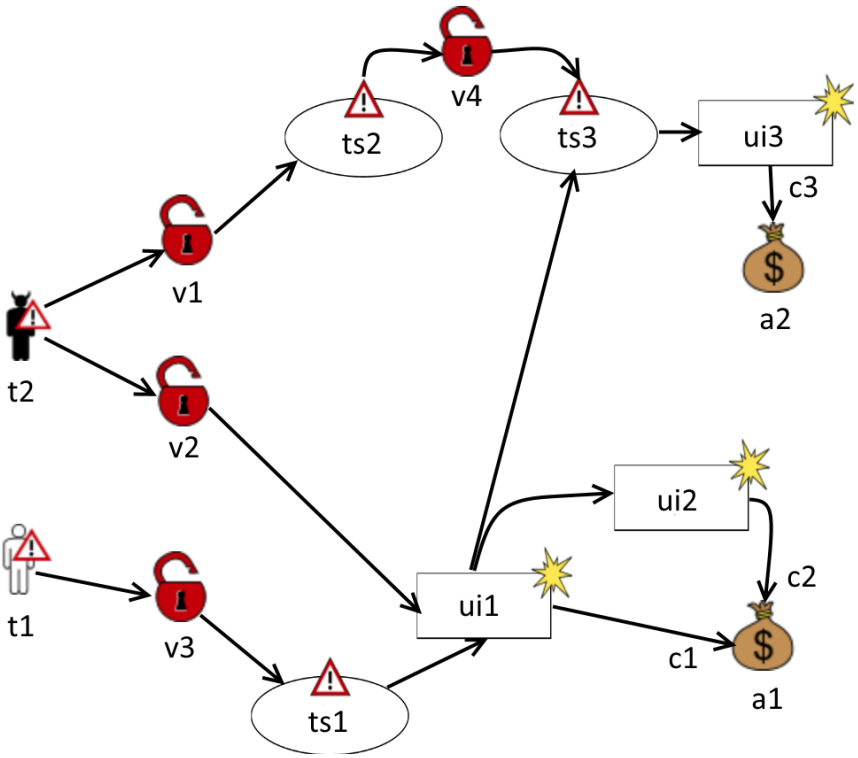


Рис. 5.2. Вид диаграммы угроз

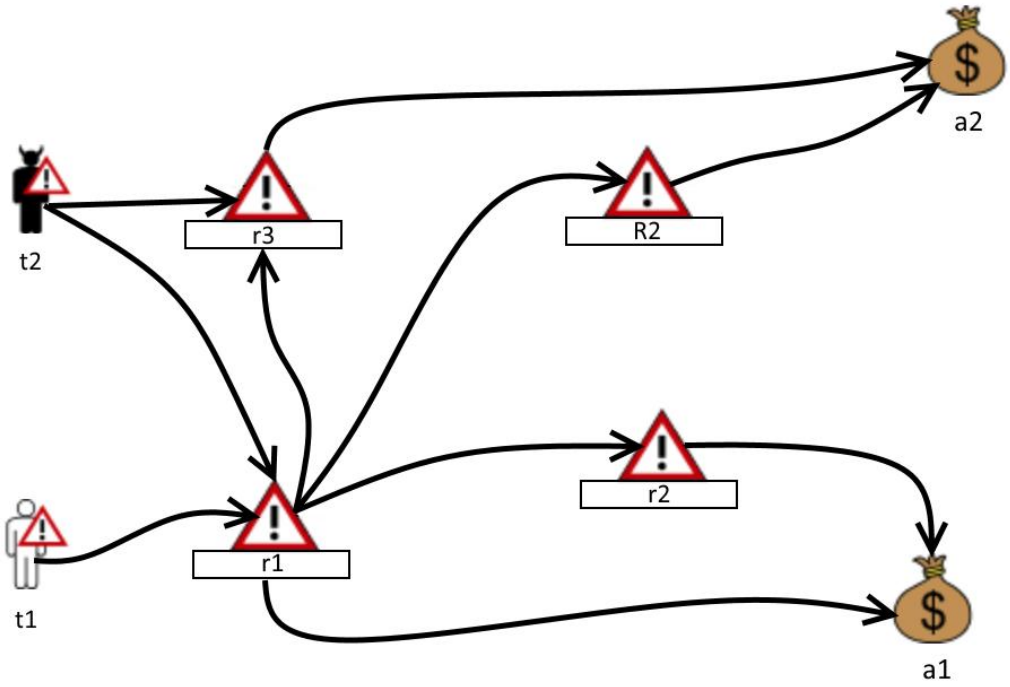


Рис. 5.3. Вид диаграммы рисков

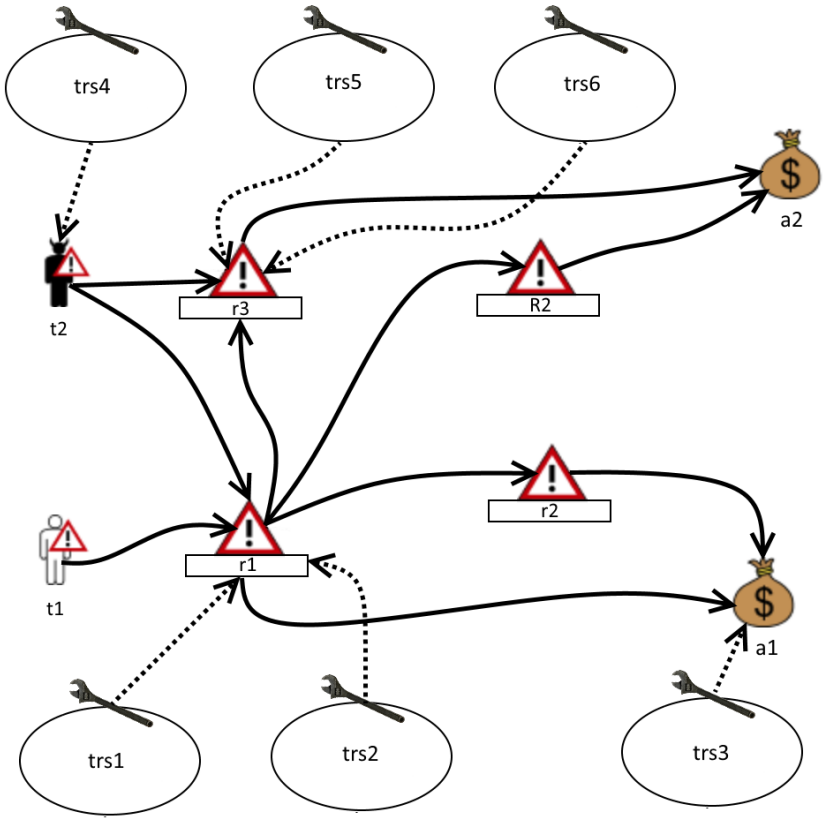


Рис. 5.4 – Вид диаграммы устранения рисков

Контрольные вопросы

1. Каким образом формализуется информация об ИС при применении методики CORAS?

2. Как определяются прямые и косвенные ресурсы и в чем их различие?

3. Для чего ресурсы сортируются в порядке их важности в ИС?

4. Каким образом вычисляются допустимые и требующие оценки риски?

5. Укажите недостатки методики CORAS.

Порядок выполнения работы

1. Выбрать вариант задания согласно Приложению Д.

2. Обобщить информационные ценности моделируемой ИС и возможные угрозы.

3. Для моделируемой ИС построить UML-диаграммы ценностей и угроз при помощи средств CORAS tools.

4. Определить уязвимости, сценарии угроз и нежелательных инцидентов. Построить UML-диаграмму угроз, которая отображает сценарии этих угроз.

5. Проанализировать риски ИС. Для этого необходимо разработать шкалу влияния рисков на моделируемую ИС и построитьUML-диаграмму угроз с вероятностями и оценками. Для рисков необходимо построить вероятностную шкалу.

6. Определить критерии оценки рисков. Построить матрицу оценки рисков, в качестве осей у которой используются значения вероятностей и последствий рисков.

7. Определить значения рисков с помощью матрицы оценки рисков.

8. Построить UML-диаграмму угроз для идентифицированных рисков.

9. Найти методы по устранению неприемлемых рисков.

10. Построить UML-диаграмму устранения рисков.

Содержание отчета

1. Формулировка задачи.

2. Исходная модель ИС.

3. Результаты анализа рисков, в том числе: UML-диаграммы обобщений информационных ценностей и угроз; UML-диаграмма угроз, которая отображает сценарии этих угроз; шкала влияния рисков на моделируемую ИС; UML-диаграмма угроз с вероятностями и оценками; вероятностная шкала для рисков; матрица оценки рисков; UML-диаграмма угроз для идентифицированных рисков; UML-диаграмма устранения рисков.

4. Ответы на контрольные вопросы.

5. Выводы по работе.

Поскольку работа в большой степени использует принципы анализа информационных потоков, угроз и уязвимостей, рассмотренных в соответствующих работах, суть ее заключается в UML-моделировании ИС с последующей автоматической обработкой такого представления.

ЛИТЕРАТУРА

1. Международный стандарт ISO/IEC 27001 «Информационные технологии. Методы безопасности. Системы управления информационной безопасностью – Требования».
2. Аверченков В.И., Рытов М.Ю., Кондрашин Г.В., Рудановский М.В. Системы защиты информации в ведущих зарубежных странах: учебное пособие для вузов. - 3-е изд., стер. - М.: Флинта, 2011. - 224 с. Режим доступа: http://www.biblioclub.ru/book/93351/
3. Варфоломеев А.А. Управление информационными рисками: Учеб. пособие. – М.: РУДН, 2008. – 158 с.
4. Милославская Н.Г. Управление рисками информационной безопасности: учеб. пособие / М.Ю. Сенаторов, А.И. Толстой, Н.Г. Милославская. – М.: Горячая линия – Телеком, 2013. – 131 с. – (Вопросы управление информационной безопасностью)
5. Киселева И.А., Искаджян С.О. Информационные риски: методы оценки и анализа // ИТ-портал, 2017. №2(14). URL: http://itportal.ru/science/economy/informatsionnye-riski-metody-otsenk/
6. Набатова Д.С. Математические и инструментальные методы поддержки принятия решений: учебник и практикум для бакалавриата и магистратуры / Д.С. Набатова. – М.: Издательство Юрайт, 2017. – 292 с. – URL: https://www.biblio-online.ru/book/0AB93023-5D55-4432-B8F1-34FE55F7BE10
7. Калинин М.О. Теория и системы управления информационной безопасностью. Анализ рисков информационной безопасности. Лабораторный практикум. – СПб.: Издательство Политехнического университета, 2010.
8. Баранова Е.К., Барабаш А.В. Моделирование системы защиты информации. – М.: РИОР ИНФРА-М, 2014. – 120 с.

СПИСОК УСЛОВНЫХ СОКРАЩЕНИЙ

ИБ – информационная безопасность
ИС – информационная система
ИТ – информационные технологии
ПО – программное обеспечение

ПРИЛОЖЕНИЕ А

Практическая работа № 1

Шаблон отчета

Состав подгруппы

_____
_____
_____
_____

1. Оценка значимости мнений экспертов

1) Критерии оценки значимости мнений экспертов и шкалы оценок:

I. Профессиональный опыт в области_____
0 – нет опыта,
1 – имеет общее теоретическое представление,
2 – имеет опыт в смежных областях деятельности,
3 – имеет практический опыт в данной области;

II. Общая эрудиция_____
0 – практически неграмотен
1 – имеет элементарные знания
2 – узкий специалист
3 – эрудит

III. Теоретические знания в области _____
0 – не имеет представления о проблеме,
1 – представляет теорию _____
2 – поверхностно изучал _____
3 – глубоко изучал теорию _____

IV. _____
0 –
_____
1 –
_____
2 –
_____
3 –_____

2) Оценка значимости критериев компетентности экспертов

Таблица 1.1– Ранжирование критериев компетентности экспертов

Критерии	I	II	III	IV
Ранги				

Таблица 1.2–Расчет рангов критериев (обобщение мнений экспертов)

Эксперт	Критерии				
	(I)	(II)	(III)	(IV)	
Сумма рангов					
Вспомогательный расчет					
Вес критерия					

3) Оценка весов значимости мнений экспертов

Таблица 1.3 – Оценка компетентности экспертов

Оцениваемые	Критерии			
	I ( )	II ( )	III ( )	IV ( )

Таблица 1.4 – Сводная таблица расчетов рангов экспертов

Оцениваемые	Критерии				Сумма рангов	Вес мнения эксперта
	I ( )	II ( )	III ( )	IV ( )		
ИТОГО						

3.Возможные риски

Таблица 1.5 – Возможные риски

№ п/п	Риск	Код риска

3. Оценка критериев значимости рисков

1) Список критериев важности рисков

(1) Возможность возникновения рисковой ситуации

(2) _____

_____

(3) _____

_____

(4) _____

_____

2) Ранжирование критериев важности рисков

Таблица 1.6 – Ранжирование критериев важности рисков

Критерии	I	II	III	IV
Ранги				

3) Расчет рангов и весов критериев важности рисков

Таблица 1.7 – Расчет рангов и весов критериев важности рисков

Эксперт	Ранг	Критерии				Сумма
		(1)	(2)	(3)	(4)	
Ранг						
Вспомогательный расчет						
Вес критерия						

4. Ранжирование рисков по критериям

1) Оценка рисков по критериям (индивидуальное мнение)

Таблица 1.8 – Оценка рисков по критериям (индивидуальное мнение)

Код риска	Критерии				Ранг
	(1)	(2)	(3)	(4)	
(1)					
(2)					
(3)					
(4)					
(5)					
(6)					
(7)					
(8)					
(9)					
(10)					
……					
(20)					

2) Оценка рисков по критериям (коллективное мнение)

Таблица 1.9 – Оценка рисков по критериям (коллективное мнение)

Код риска	Эксперты и вес их мнения				Расчетный ранг	Приоритет
(1)						
(2)						
(3)						
(4)						
(5)						
(6)						
(7)						
(8)						
(9)						
(10)						
(11)						
(12)						
(13)						
(14)						
(15)						
(16)						
(17)						
(18)						
(19)						
(20)						

5. Составление перечня 10 важнейших рисков

Таблица 1.10 – Десять важнейших рисков

Приоритет риска	Код риска	Сущность риска
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Выводы и рекомендации:

Варианты заданий к практической работе № 1

Вариант № 1. ООО «Луч - С» представляет собой сеть магазинов бытовой техники. Магазины пользуются успехом у покупателей: объемы реализации стабильно большие, есть постоянные клиенты, оборачиваемость товаров достаточно высокая. Успех компании, по мнению менеджеров, заключался в том, что потребителям предлагались только проверенные и хорошо зарекомендовавшие себя товары известных отечественных и зарубежных производителей бытовой техники, изготовленные в ведущих производственных подразделениях фирм («белая сборка»). Другими факторами успеха ООО «Луч - С» стали расположение магазинов в центрах спальных районов, собственная система поставок, не привлекая посредников и собственный сервисный центр. Все работники магазинов имели гибкую систему оплаты, включающую стабильный социальный пакет и заработную плату, пропорциональную выручке от реализации по данному подразделению.

Однако в городе появилось ОАО «Форсаж», работающее в том же сегменте рынка. ОАО проводит агрессивную стратегию, копируя все удачные стратегические решения ООО «Луч - С» и переманивая покупателей дисконтными картами и распродажами. Сокращения объемов реализации ООО пока не произошло, но темпы роста выручки заметно упали.

В дирекцию ООО поступило предложение сервисного центра: закупать у производителей техники только комплектующие, а сборку бытовой техники осуществлять на месте, что снизит себестоимость за счет сокращения транспортных расходов (компактность размещения грузов) и таможенных пошлин (комплектующие имеют более низкую ставку, чем готовые изделия, кроме того, комплектующие дешевле техники в сборе). Это обеспечило бы снижение издержек не менее чем на 20 % и стало бы существенным конкурентным преимуществом ООО «Луч - С». Возможность подобного решения обеспечивается также многолетними связями с фирмами производителями техники, где ООО имело положительную деловую репутацию.

Но для реализации проекта необходимо создание собственного сборочного производства.

Вариант № 2. В престижный салон-парикмахерскую «Твой стиль» обратилась известная российская косметическая фабрика «Марьяна» с предложением о развитии партнерства. В соответствии с предлагаемым договором, «Марьяна» поставляет косметические товары (как для использования в салоне, так и для продажи клиентам) со скидкой от 50 % до 75 %, а в ответ «Твой стиль» обязуется применять исключительно косметические средства этой фабрики и вести статистику за уровнем потребления и собирать критические замечания в адрес конкретных товаров.

Косметическая фабрика производит весь спектр необходимой косметики для ухода за волосами, продукция компании достаточно популярна, однако последние инновации оказались несколько менее рентабельными, чем предполагалось ранее, в результате по ценовому диапазону средства «Марьяна» почти сравнялись по стоимости с западными аналогами. Договор с «Твой стиль» способствовал бы росту сбыта продукции. Кроме того, обратная связь с потребителями могла бы дать идею относительно будущего развития товаров под маркой «Марьяна».

Часть мастеров салона предпочитают работать с косметикой западного производства, утверждая, что это – требование клиентов. Кроме того, на парикмахеров возлагается дополнительная обязанность «разговорить» клиента и зафиксировать его мнение о новых косметических средствах.

Руководство салона-парикмахерской видит положительные стороны сотрудничества в прямой материальной выгоде: возможно снижение издержек и проведение рекламной кампании под девизом: «Россиянину – лучшее российское».

ПРИЛОЖЕНИЕ Б

Варианты заданий к практической работе № 2

Вариант 1**.** Инновационный проект предусматривает развитие сбытовой сети. Согласно одному из предложений, предусмотрено создание сети собственных фирменных магазинов. Затраты на рекламу и маркетинг по смете составляют 120 млн руб., затраты на содержание 1 магазина 500 тыс. руб. Планируется открытие 10 магазинов. Исследования показали, что создание собственной сети предоставляет возможность гарантировать сбыт продукции на уровне 70 %. Предложение заключить договор с 2 оптовыми распространителями предоставляет возможность повысить гарантированность сбыта до 100 %. Договор с оптовиками предусматривает скидку к цене в размере 25 %. Надежность каждого из поставщиков оценивается на уровне 95 %. В случае форс-мажорных обстоятельств один из оптовиков способен дополнительно реализовать не более 50 % первоначального договора. Сравните обе альтернативы методом «дерева решений», если объем реализации запланирован на уровне 30 млрд руб. при себестоимости 15 млрд руб. Налоги не учитывать.

Вариант 2. На вакантную должность руководителя проекта претендуют два кандидата: выпускник ГУУ, закончивший вуз с отличием («теоретик»), и претендующий на более высокую должность сотрудник фирмы-конкурента («практик»). Теоретик готов работать в компании за 500 у. е. в месяц, однако отсутствие реальной практики повышает риск принятия ошибочных управленческий решений до 10 %. Практик требует заработной платы в размере 1500 у.е. в месяц, а вероятность ошибки при принятии управленческих решений составляет 1 %. Срок контрактов в обоих случаях 1 год. В среднем за год руководитель проекта принимает 250туправленческих решений. В среднем, каждое правильное решение приносит компании 200 у.е. прибыли. На каждом ошибочном решении компания теряет в среднем 250 у.е. Также можно обратиться в кадровое агентство, которое готово найти «среднюю кандидатуру» (оклад 1000 у.е. в месяц, ошибки в 5 случаях из 100). Услуги кадрового агентства 3000 у.е. Обоснуйте кадровое решение методом «дерева решений».

Вариант 3. Обоснуйте выбор альтернативы методом «дерева решений» в случае, если для сопровождения инновационного проекта требуется реализация на рынке трехфазного интегратора. Можно организовать собственную сборку аппарата (стоимость реализации подпроекта300 млн. руб.). В данном случае появляются технологические проблемы освоения производства, которые приводят к выпуску бракованных изделий на уровне 10%. При этом в 1 случае из 200 брак неустраним. Устранение брака приводит к росту себестоимости на 20 %. Себестоимость интегратора 200 тыс. руб. Также можно заключить договор поставки интеграторов из Китая по закупочной цене 300 тыс. руб. Надежность поставщика 98 %. Потери от недопоставки интеграторов 700 млн руб. Потребность в интеграторах оценивается на уровне1500 шт. в год.

ПРИЛОЖЕНИЕ В

Варианты заданий к практической работе № 3

Вариант 1. Тестовая информационная система ЗАО "ТестИС-Строй".

Основной вид деятельности ЗАО "ТестИС-Строй" – продажа строительных товаров на рынке "BusinesstoClient". Поставщиками являются частные лица и организации среднего и малого бизнеса. ЗАО "ТестИС-Строй" имеет четыре точки продаж, расположенные в пределах города. Каждая из этих точек – магазин площадью от 300 до2000 м^2. В каждом магазине работает до 100 сотрудников.

ЗАО "ТестИС-Строй" имеет центральный офис в центре города, где располагается дата-центр, включающий центральную базу данных товаров и серверы баз данных бухгалтерии, отдела кадров и т. д. В центральном офисе и на каждой из точек продаж развернуты локальные вычислительные сети (ЛВС). Каждая из ЛВС точек продаж связана с центральным офисом посредством сети Интернет. В точках продаж функционируют 1-2 сервера, обеспечивающих синхронизацию с центральной базой данных, и до 20 рабочих станций: компьютеры директора магазина, секретаря, терминалы в торговых залах.

В дата-центре установлены Web-сайт электронного магазина и почтовый сервер.

К терминалам торговых залов исключена возможность подключения внешних носителей. В дата-центре все серверы размещены в несгораемых сейфах, доступ в помещение контролируется физически(охраняемое помещение). В торговых точках все серверы находятся в кабинетах, закрываемых на ключ. На всех компьютерах, кроме терминалов в торговых залах, установлено антивирусное ПО.

На серверах дата-центра установлен межсетевой экран. На сервере базы данных бухгалтерии дополнительно установлена система обнаружения вторжений.

Для подключения к дата-центру используется защищенноеVPN-соединение. Для подключения к центральной базе товаров предусмотрен резервный канал. Загрузка терминалов торговых залов обеспечивается только после введения пароля в BIOS.

Вариант 2. Тестовая информационная система издательства газеты "ТестИС-Пресс".

Редакция газеты ТестИС-Пресс" занимается публикацией новостей из мира информационных технологий.

Читатели и конкуренты не должны иметь возможности узнать о публикуемых новостях ранее выпуска номера (факторы актуальности и эксклюзивности).

Издательство "ТестИС-Пресс" включает подразделения: руководство (директор и заместитель, главный редактор), IT-отдел (администраторы),

бухгалтерия (главный бухгалтер и бухгалтеры),журналисты, редакторы, наборщики, верстальщики. Типография также входит в состав издательства (сотрудниками являются инженеры по печати и переплету). Всего в редакции работают 60 сотрудников.

В бухгалтерии используются два сервера: для хранения бухгалтерской базы данных и ее резервных копий. Каждый редактор, журналист, наборщик и верстальщик работает на своей рабочей станции. В издательстве используется несколько серверов: для хранения материалов готовящегося к выходу номера, хранения архивов номеров. Почта и web-сайт издательства функционируют на двух выделенных серверах. Доступ в Интернет осуществляется через Провайдера. Издательство готово к сотрудничеству с внешними аудиторами.

В издательстве используется система криптозашиты электронной почты. На рабочих станциях редакторов и журналистов настроена система автоматической блокировки станции при отсутствии сотрудника на рабочем месте. В бухгалтерии установлена система видеонаблюдения. Доступ в серверную комнату обеспечивается только по пропускам. Предусмотрено резервное копирование бухгалтерской базы данных.

Вариант 3. Тестовая информационная система компании по обслуживанию средств электронной коммерции "ТестИС-Е".

Компания "ТестИС-Е" осуществляет деятельность в рамках продаж и обслуживания оборудования электронной коммерции.

В компании существуют три отдела: бухгалтерия (главный бухгалтер, бухгалтеры), отдел технического анализа (руководитель отдела, инженеры), отдел продаж (руководитель отдела, заместитель, менеджеры). Для всех сотрудников предоставлена рабочая станция с выходом в Интернет. В конференц-зале установлена рабочая станция (ноутбук), которую используют только члены совета директоров (финансовый директор, генеральный директор и его заместитель). В компании определена должность администратора, имеющего доступ ко всем ресурсам системы за исключением сервера коммерческих данных.

В отделе технического анализа расположен сервер-хранилище информации. Доступ к нему имеют только сотрудники этого отдела.

Почтовым сервером, расположенным в серверном помещении, пользуются сотрудники отдела продаж, дирекция и бухгалтерия. К серверу коммерческих данных, расположенному в серверном помещении, имеют доступ только члены совета директоров и главный бухгалтер (администратор не имеет доступа к этому серверу). Резервное копирование этого сервера выполняется на CD-R-носители, хранимые в сейфе генерального директора.

Для доступа в Интернет используется шлюз в виде отдельного сервера, размещенного в серверном помещении. На нем установлена служба VPN-доступа, Web-прокси, служба фильтрации запросов, система учета трафика и система обнаружения вторжений.

В компании не используется антивирусное программное обеспечение. Внутренние документы и настройки безопасности рабочих станций запрещают запускать любые программы, кроме, установленных на компьютерах. Запрещена инициация соединений с рабочими станциями пользователей внешней сети. На почтовом сервере используется система антивирусной защиты электронной почты и защиты от спама.

Вариант № 4. Тестовая информационная система компании по разработке программного обеспечения "ТестИС-Солюшн".

Компания "ТестИС-Солюшн" занимается разработкой программного обеспечения, используемого в банках. Руководство компании "ТестИС-Солюшн" представлено генеральным директором, его заместителем и техническим директором. Штатный состав компании составляет 70 человек.

Разработки компании имеют закрытый тип. Для их контроля и контроля используемых ресурсов в штатном расписании предусмотрены следующие должности: главный администратор, администратор файловых серверов, сетевой администратор. Остальные сотрудники – инженеры по разработке ПО, тестировщики, разработчики и руководители проектов. В бухгалтерии работает один человек – главный бухгалтер. База данных бухгалтерии находится на его рабочей станции. Информация, обрабатываемая в системе – результаты и данные разработки программных продуктов: исходные коды, документация, результаты тестирования.

В компании используется антивирусная защита, все серверы расположены в серверном помещении, закрываемом на ключ. На серверах установлены системы контроля версий; почтовый и файловый серверы защищены межсетевым экраном. Сервер системы контроля версий доступен тестировщикам из Интернет по VPN-соединению. Компьютер главного бухгалтера не имеет дисководов и устройств подключения USB, кроме того, он не включен в основную сеть. Резервное копирование не производится. Дирекция и руководители проектов имеют доступ в Интернет с рабочих мест. Только разработчики могут вносить изменения в систему контроля версий.

ПРИЛОЖЕНИЕ Г

Варианты заданий к практической работе № 4

Вариант 1. Совокупная стоимость активов организации составляет 100 000 у.е. На учредительном собрании руководство приняло решение о реализации перспективного направления в производстве. Для нового отдела были закуплены 10 персональных компьютеров, каждый стоимостью 400 у.е. На каждый компьютер было установлено программное обеспечение стоимостью 300 у.е. на один компьютер. Для обеспечения доступа всего отдела к локальной сети организации дополнительно потрачено 1000 у.е. на закупку сетевого оборудования. Вероятность сетевого вторжения составляет 40 % для данного региона. Среднее количество сетевых вторжений в данном регионе составляет 3 раза в год. На обеспечение зашиты компьютерной сети отдела планируется выделить 800 у.е.

Вариант 2. Совокупная стоимость активов организации составляет 35 000 у.е. В организации есть база данных (БД) заказчиков, которая содержит ценную информацию. Стоимость аналогичной БД на рынке составляет 5000 у.е. Но если данная БД будет украдена и произойдет публичная продажа, что весьма вероятно, то в этом случае ее стоимость снизится до 100 у.е. Вероятность кражи БД составляет 30 %. Для обеспечения зашиты БД было затрачено1000 у.е.

Вариант 3. В организации купили новые серверы для того, чтобы обеспечить доступ в Интернет. В организации работают 300 сотрудников, трудозатраты каждого из них в среднем равны 30 у.е./ч. После реализации сетевого вторжения на восстановление системы в среднем необходимо потратить 5 часов. В организации есть БД заказчиков, которая содержит ценную информацию. Стоимость аналогичной БД на рынке составляет 3000 у.е. Но если данная БД будет украдена и произойдет публичная продажа, что весьма вероятно, то в этом случае стоимость снизится до 100 у.е. Вероятность кражи БД составляет 20 %. Среднее количество краж в данном регионе составляет 2 раза в год. Организация решила закупить антивирусное программное обеспечение на общую сумму 2000 у.е. для защиты всех серверов и компьютеров.

Вариант 4. В организации купили беспроводные маршрутизаторы для организации беспроводного доступа к локальной сети. В связи с этим часть организации перешла на беспроводную связь. В организации работают 100 сотрудников, трудозатраты каждого из них в среднем равны 30 у.е./ч. Изменения в ИС приводят к повышению вероятности реализации вирусной угрозы на 20 %, а на полное восстановление ИС в случае заражения в среднем необходимо потратить 3 часа. Организация решила закупить антивирусное программное обеспечение для защиты серверов и компьютеров на сумму 1000 у.е.

ПРИЛОЖЕНИЕ Д

Варианты заданий к практической работе № 5

Примечание: если в варианте задания не указана операционная система, то не имеет значения, какая система установлена.

Вариант 1. Система состоит из двух серверов, которые используют для доступа в глобальную сеть общий браузер.

Вариант 2. Сотрудники предприятия, занимающиеся разработкой программного обеспечения, используют web-приложения. На каждом компьютере они работают с важной информацией, потеря которой является критичной.

Вариант 3. Электронная коммерция в сфере услуг: покупка и оплата товара в интернет-магазине.

Вариант 4. Три сервера объединены в общую сеть с выходом в Интернет. На двух серверах установлен межсетевой экран, а на третьем – только антивирусное оборудование.

Вариант 5. Локальная сеть состоит из четырех компьютеров. На каждом компьютере установлены антивирус и система обнаружения вторжений.

Вариант 6. В операционной системе Windows четыре учетные записи пользователей, при этом три записи имеют права администратора. Пользователь под четвертой записью сам получает права администратора принудительно в процессе работы системы.

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ И ПРОГНОЗИРОВАНИЕ ИНФОРМАЦИОННЫХ УГРОЗ

Часть 1

АНАЛИЗ ИНФОРМАЦИОННЫХ РИСКОВ

Учебно-методическое пособие

Составители: **Маслова** Мария Александровна, **Шумейко** Ирина Петровна

В авторской редакции

Изд. № 120/18. Объем 3,75 п.л.
РИИЦМ ФГАОУ ВО «Севастопольский государственный университет»