ВЫСШЕЕ ОБРАЗОВАНИЕ — БАКАЛАВРИАТ

серия основана в 1996 г.

Е.К. БАРАНОВА
А.В. БАБАШ

МОДЕЛИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

ПРАКТИКУМ

УЧЕБНОЕ ПОСОБИЕ

Рекомендовано Учебно-методическим объединением по образованию в области прикладной информатики в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению «Прикладная информатика»

Электронно-Библиотечная Система
znanium.com

Соответствует Федеральному государственному образовательному стандарту 3-го поколения

Москва
РИОР
ИНФРА-М

УДК 621.391+004.9(075.8)
ББК 32.81я73
Б24

ФЗ № 436-ФЗ	Издание не подлежит маркировке в соответствии с п. 1 ч. 1 ст. 11

Авторы: *Баранова Елена Константиновна*, доцент кафедры информационной безопасности НИУ «Высшая школа экономики» (Москва); *Бабаш Александр Владимирович*, профессор кафедры информационной безопасности НИУ «Высшая школа экономики» (Москва)

Рецензенты: кафедра комплексного обеспечения информационной безопасности Московского государственного университета экономики, статистики и информатики (Москва), зав. кафедрой *Баяндин Н.И.*; кафедра информационной безопасности и программной инженерии Российского государственного социального университета (Москва), канд. техн. наук, доцент *Хорев П.Б.*

Баранова Е.К., Бабаш А.В.

Б24 Моделирование системы защиты информации. Практикум: Учеб. пособие. — М.: РИОР: ИНФРА-М, 2015. — 120 с. + Доп. материалы [Электронный ресурс; Режим доступа http://www.znanium.com].— (Высшее образование: Бакалавриат). — www.dx.doi.org/10.12737/5071.

ISBN 978-5-369-01379-3 (РИОР)
ISBN 978-5-16-010205-4 (ИНФРА-М, print)
ISBN 978-5-16-102078-4 (ИНФРА-М, online)

В пособии рассматриваются задачи проектирования и оценки эффективности системы защиты информации (СЗИ) с использованием различных методов моделирования. Рассматриваются задачи и программный инструментарий для их решения — проектирование с использованием модели с полным перекрытием множества угроз; анализ и управление рисками информационной безопасности (ИБ) с использованием программного пакета CORAS и программного комплекса ГРИФ; система поддержки принятия парето-оптимальных решений в области проектирования СЗИ; разработка сценариев действий нарушителя ИБ с использованием сети Петри; определение показателей защищенности информации при несанкционированном доступе.

Практикум может быть рекомендован бакалаврам и магистрам, изучающим курсы «Информационная безопасность» и «Управление информационной безопасностью», а также смежные с ними дисциплины.

УДК 621.391+004.9(075.8)
ББК 32.81я73

Материалы, отмеченные знаком ,
доступны в электронно-библиотечной системе ZNANIUM
по адресу http://znanium.com.
Ссылку для доступа вы можете получить
при сканировании QR-кода, указанного на обложке

ISBN 978-5-369-01379-3 (РИОР)
ISBN 978-5-16-010205-4 (ИНФРА-М, print)
ISBN 978-5-16-102078-4 (ИНФРА-М, online)

© Баранова Е.К., Бабаш А.В., 2015

ПРЕДИСЛОВИЕ

Информационная безопасность является одной из главных проблем, с которой сталкивается современное общество. Причиной обострения этой проблемы является широкомасштабное использование автоматизированных средств накопления, хранения, обработки и передачи информации.

Решение проблемы информационной безопасности связано с гарантированным обеспечением трех ее главных составляющих: *доступности*, *целостности* и *конфиденциальности информации*.

Важную роль при построении системы информационной безопасности играют процесс моделирования и анализ предлагаемых моделей.

Моделирование системы информационной безопасности заключается в построении образа системы, с определенной точностью воспроизводящего процессы, происходящие в реальной системе. Для моделирования процессов в системе защиты информации используются различные методы.

Аналитическое моделирование предполагает рассмотрение функционирования исследуемой системы в виде математических или логических соотношений. Для этих целей используется мощный математический аппарат: алгебра, функциональный анализ, разностные уравнения, теория вероятностей, математическая статистика, теория множеств и другие.

Имитационное моделирование предполагает представление моделируемой системы в виде некоторого аналога реальной системы. В процессе имитационного моделирования на компьютере реализуются алгоритмы изменения основных характеристик реальной системы в соответствии с эквивалентными реальным процессам математическими и логическими зависимостями.

Для моделирования систем информационной безопасности целесообразно использовать следующие теории и методы, позволяющие свести решение задачи к формальным алгоритмам:

- теория нечетких множеств;
- теория конфликтов;
- теория графов;
- формально-эвристические методы;
- эволюционное моделирование.

В предлагаемом читателю практикуме по моделированию системы защиты информации на предприятии рассматриваются задачи и программный инструментарий для их решения, в частности, проектирование систем защиты информации с использованием модели с полным перекрытием множества угроз; анализ и управление рисками информационной безопасности с использованием программного пакета CORAS и программного комплекса ГРИФ; система поддержки принятия парето-оптимальных решений в области проектирования системы защиты информации; разработка сценариев действий нарушителя информационной безопасности с использованием сети Петри; определение показателей защищенности информации при несанкционированном доступе.

Все практические задания снабжены соответствующим теоретическим материалом, программным инструментарием для выполнения работы, контрольными вопросами по темам, требованиями к отчету по проведению работы и вариантами заданий.

Практикум может быть рекомендован бакалаврам и магистрам, изучающим курсы «*Информационная безопасность*» и «*Управление информационной безопасностью*», а также смежные с ними дисциплины.

Все практические работы были неоднократно опробованы авторами в учебном процессе на кафедре информационной безопасности НИУ «Высшая школа экономики».

Авторы выражают благодарность студентам Российского государственного социального университета Юлии Жуковой, Михаилу Медведеву и Игорю Ларионову за подготовку и тестирование программного инструментария для проведения практических работ.

1. ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ МОДЕЛИ С ПОЛНЫМ ПЕРЕКРЫТИЕМ МНОЖЕСТВА УГРОЗ

Цель практической работы: исследование возможностей графового моделирования для анализа рисков информационной безопасности объекта информатизации, в частности, изучение принципов построения двудольных и трехдольных графов с полным перекрытием множества угроз безопасности.

Для выполнения практической работы на компьютере необходимо запустить программу из папки: *Исполняемые модули/1_Модель с полным перекрытием угроз.*

1.1. Описание модели безопасности с полным перекрытием множества угроз

Модель безопасности с полным перекрытием, разработанная в 1970-х гг., строится исходя из постулата, что система безопасности должна иметь, по крайней мере, одно средство для обеспечения безопасности на каждом возможном пути воздействия нарушителя на информационную систему.

В модели точно определяется каждый объект, требующий защиты, оцениваются средства обеспечения безопасности в отношении их эффективности и их вклад в обеспечение безопасности всей информационной системы. С каждым объектом, требующим защиты, связывается некоторое множество действий, к которым может прибегнуть нарушитель для получения несанкционированного доступа к объекту.

Множество отношений «объект-угроза» образует двудольный граф, в котором ребро (y_i, o_j) существует тогда и только тогда, когда y_i является средством получения доступа к объекту o_j. Пример модели процесса защиты информации в виде двудольного графа приведен на рис. 1.1.

Следует отметить, что связь между угрозами и объектами не является связью типа «один к одному» — угроза может распространяться на любое число объектов, а объект может быть уязвим со стороны более чем одной угрозы. Цель защиты состоит в том, чтобы «перекрыть»

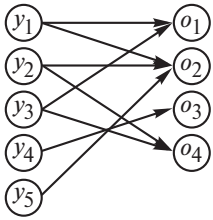


Рис. 1.1. Пример модели процесса защиты информации в виде двудольного графа

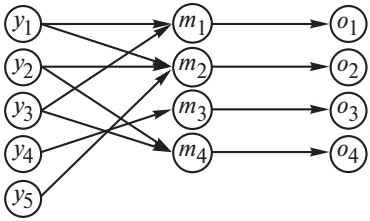


Рис. 1.2. Пример модели процесса защиты информации в виде трехдольного графа

каждое ребро данного графа и воздвигнуть барьер для доступа по этому пути.

В идеальном случае каждое средство защиты $m_k \in M$ должно устранять некоторое ребро (y_i, o_j). В действительности m_k выполняет функцию «барьера», обеспечивая некоторую степень сопротивления попыткам проникновения.

Набор M средств обеспечения безопасности преобразует двудольный граф в трехдольный. На рис. 1.2 приведен пример модели процесса защиты информации в виде трехдольного графа.

Ребра указывают на соответствующие связи между угрозами, средствами защиты и множеством объектов защиты.

Система обеспечения безопасности описывается в виде пятикортежного набора

$$S = \{O, Y, M, V, B\},$$

где O — набор защищаемых объектов;

Y — набор угроз;

M — набор средств обеспечения безопасности;

V — набор уязвимых мест — отображение $T \times O$ на набор упорядоченных пар $V_i = (y_i, o_j)$, представляющих собой пути проникновения в систему;

B — набор барьеров — отображение $V \times M$ или $T \times O \times M$ на набор упорядоченных троек $b_i = (y_i, o_j, m_k)$, представляющих собой точки, в которых требуется осуществлять защиту в системе.

Модель системы безопасности с полным перекрытием описывает требования к составу подсистемы защиты объекта информатизации. Но в ней не рассматривается вопрос стоимости внедряемых средств защиты и соотношения затрат на защиту и получаемого эффекта. Кроме того, определить полное множество «путей проникновения» в систему на практике может оказаться достаточно сложно.

Анализ графа дает возможность оценить, все ли возможные пути реализации угроз перекрыты, и выработать рекомендации в случае отсутствия защиты каких-либо объектов. Заметим, что математический аппарат для анализа графовых структур достаточно хорошо разработан, что позволяет проводить анализ достаточно разветвленных графов. Кроме того, процесс построения и модернизации графа легко выполняется с использованием программного обеспечения.

Отметим, что рассмотренная модель безопасности с полным перекрытием применима, в основном, как инструментарий при разработке определенных политик безопасности либо в случае построения комплексной системы защиты информации для малого предприятия, так как при большом объеме множеств *Y*, *M* и *O* анализ модели становится затруднительным.

1.2. Порядок работы с программным инструментарием

Программный модуль позволяет проводить оценку рисков информационной безопасности на основе модели безопасности с полным перекрытием множества угроз.

Для описания модели используем методологию структурного анализа *IDEF0*. Модель *IDEF0* позволяет понять, какие объекты или информация служат сырьем для процессов, какие результаты получаются, что является управляющими факторами и какие ресурсы для этого необходимы.

На контекстной диаграмме первого уровня (рис. 1.3) показаны входы и выходы, а также управление и механизмы. Эти потоки будут в дальнейшем использоваться при описании бизнес-процессов более низких уровней.

Входными данными являются множества угроз, средств защиты и объектов защиты, а также связи между объектами.

К *выходным данным проектируемой модели* относятся:

- графическое представление модели в виде трехдольного графа;
- отчет о результате анализа графа.

Управлением для проектируемой модели служит:

- список объектов модели.

Механизмом для проектируемой модели выступает:

- пользователь.

На втором уровне контекстной диаграммы (рис. 1.4) определим более подробно основные процессы проведения анализа рисков инфор-

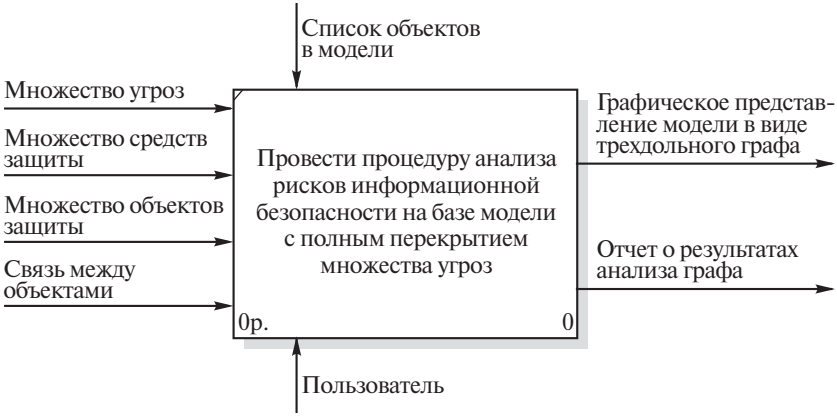


Рис. 1.3. Контекстная диаграмма А-0 «Провести процедуру анализа рисков информационной безопасности на базе модели с полным перекрытием множества угроз»

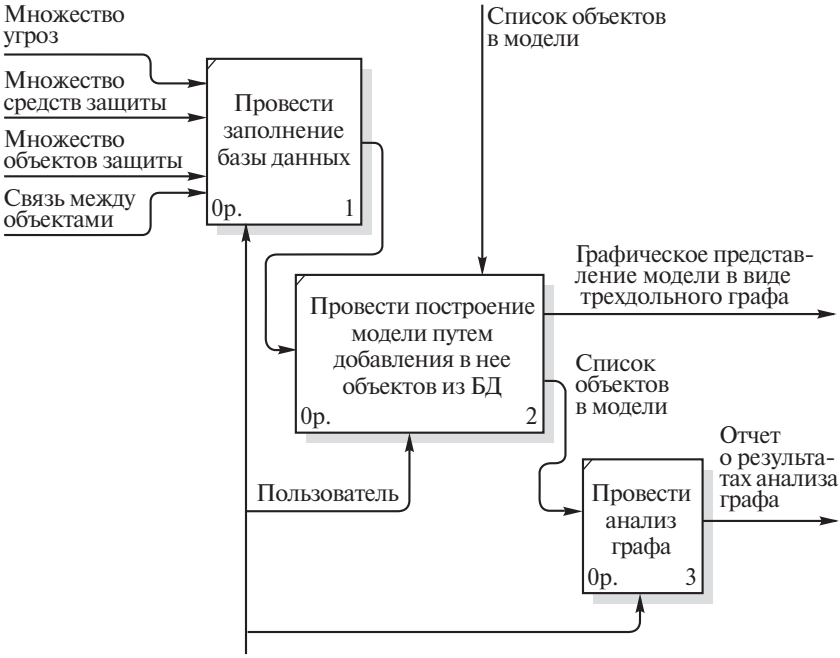


Рис. 1.4. Декомпозиция диаграммы А-0

мационной безопасности на базе модели с полным перекрытием множества угроз.

Процесс анализа рисков информационной безопасности на базе модели с полным перекрытием множества угроз посредством программного модуля состоит из следующих подпроцессов:

- заполнение базы данных;
- добавление объектов в модель;
- формирование выходного отчета.

Заполнение базы данных

Для начала работы с программным инструментарием, пользователю необходимо заполнить базу данных объектами в окне **Редактирование базы данных** (рис. 1.5). Для этого необходимо в главном меню выбрать пункт **База Данных → Редактировать БД**. Далее необходимо нажать на кнопку **Добавить**, заполнить необходимые поля и нажать кнопку **OK**. После этого в таблице отобразится новый объект. Теперь необходимо задать для него связи с другими объектами. С целью обновления списка связей нового объекта требуется вы-

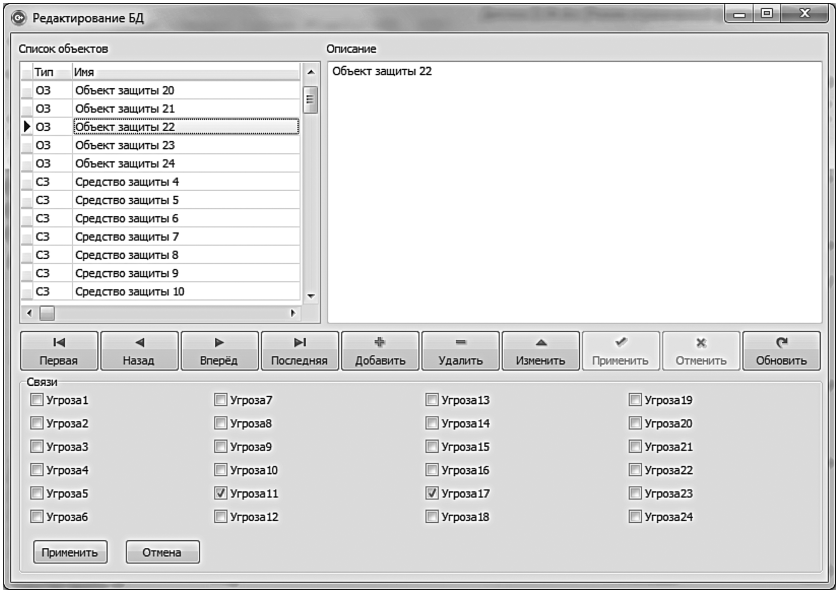


Рис. 1.5. Основная форма редактирования базы данных

брать его в таблице, после этого в нижней части окна отобразятся все объекты, для которых возможно задать связь. Следует поставить метки против тех объектов, связь с которыми требуется установить, и после этого нажать кнопку **Применить** (иначе связи сбросятся).

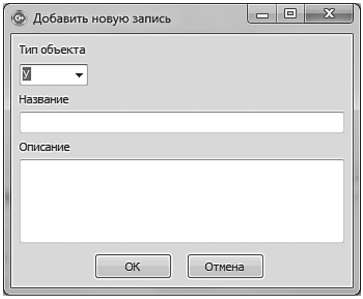


Рис. 1.6. Форма добавления новой записи в базу данных

Максимальное количество объектов каждого типа в базе банных — 24. Возможно и редактирование базы данных вручную средством *Microsoft Access*.

После нажатия кнопки **Добавить** на форме редактирования базы данных отображается форма добавления новой записи (рис. 1.6), которая позволяет выбрать тип, задать имя и описание добавляемого объекта.

Добавление объектов в модель

Следующим этапом работы с программой является добавление объектов из базы данных в модель. Это делается при помощи кнопки **Добавить в модель** в основном окне программы (рис. 1.7). Перед этим

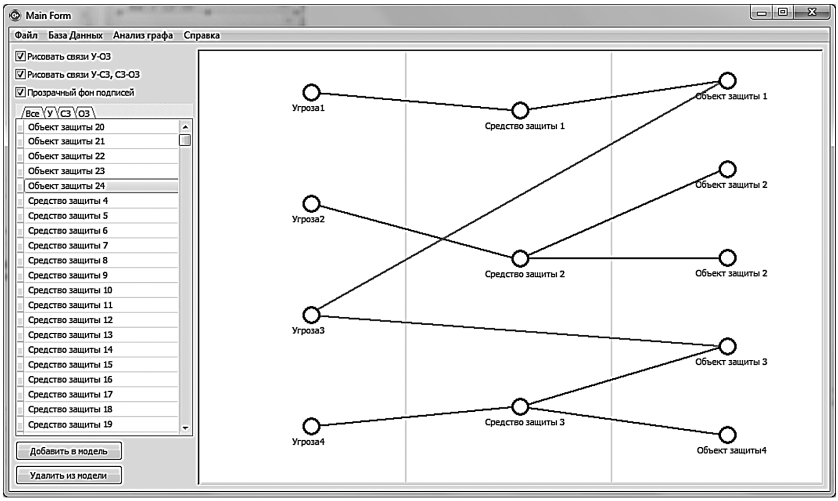


Рис. 1.7. Главное окно программы

необходимо выбрать добавляемый объект в списке в этом же окне. Возможно также и удаление объекта нажатием кнопки **Удалить из модели**. После добавления или удаления объекта изменения сразу отображаются в виде изменения отображаемого графа. Максимальное число объектов каждого типа в модели — 24. Возможно сохранение и загрузка модели в файл с помощью главного меню и пунктов **Сохранить модель**, **Загрузить модель**, а также полная очистка модели с помощью соответствующего пункта.

Формирование выходного отчета

Заключительный этап работы с программой выполняется с помощью пункта главного меню **Анализ графа**, после чего пользователю выводится форма с соответствующим отчетом.

Поскольку анализируемая модель представляет собой граф, анализировать будем вершины в графе и связи между ними. При этом отчет по результатам анализа может носить только рекомендательный характер, целью которого является лишь обратить внимание пользователя на те или иные элементы модели.

Выделим критерии оценки сформированного графа.

1. Объект защиты не имеет барьера (средства защиты), т.е. существует прямая связь «угроза—объект».
2. Угроза имеет несколько средств защиты, перекрывающих ее (можно сделать предположение об избыточности средств защиты).
3. Средство защиты имеет несколько угроз, которые оно перекрывает (можно сделать предположение о недостаточности средств защиты).

Пример отчета представлен на рис. 1.8.

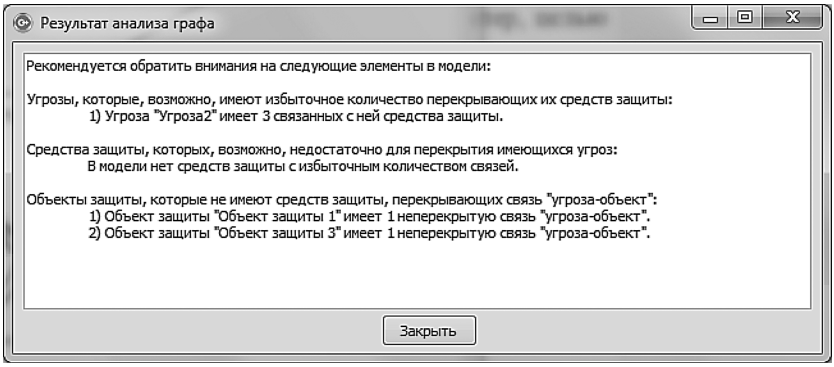


Рис. 1.8. Пример отчета, сформированного по результатам анализа графа

Необходимо также отметить возможность включения и отключения отображения некоторых связей в графе для более удобного восприятия посредством установки соответствующих «чекбоксов» в главном окне приложения.

1.3. Задания для моделирования СЗИ и требования к отчету

1. Описать структуру предприятия (варианты заданий см. Приложение 1).
2. Составить перечень объектов защиты на рассматриваемом предприятии.
3. Определить и описать полное множество угроз информационной безопасности на предложенном для анализа предприятии.
4. Заполнить базу данных для рассматриваемого варианта (угрозы, объекты защиты).
5. Построить двудольный граф (угрозы — объекты защиты). Проанализировать полученную модель. Сформулировать выводы.
6. Добавить в базу данных и описать предполагаемые средства защиты на рассматриваемом предприятии.
7. Построить трехдольный граф (угрозы — средства защиты — объекты защиты). Проанализировать полученную модель. Сформулировать выводы.
8. Скорректировать трехдольный граф для получения оптимальной схемы защиты объектов Для этого добавить в базу данных и описать необходимые средства защиты. Сформулировать выводы.
9. В отчете по практической работе должны быть представлены:

– схема и описание организации, в соответствии в полученным вариантом;
– таблица с перечнем угроз безопасности;
– таблица с перечнем объектов защиты;
– таблица с перечнем средств защиты;
– двудольный граф (угрозы — объекты защиты);
– первоначальный и скорректированный трехдольные графы (угрозы — средства защиты — объекты защиты);
– выводы по результатам анализа графов.

Контрольные вопросы и задания

1. Какие методы моделирования наиболее эффективны при построении системы защиты объекта информатизации?
2. Опишите этапы построения модели с полным перекрытием множества угроз безопасности.
3. В чем особенность, достоинства и недостатки модели с полным перекрытием множества угроз безопасности?
4. Для каких объектов оценки модель с полным перекрытием множества угроз не может применяться? Приведите аргументацию и конкретные примеры.
5. Какие выводы могут быть сформулированы на основе анализа двудольного графа модели с полным перекрытием множества угроз? Приведите конкретный пример.
6. Какие выводы могут быть сформулированы на основе анализа трехдольного графа модели с полным перекрытием множества угроз? Приведите конкретный пример.
7. На каких этапах создания защищенных информационных систем рекомендуется использование модели с полным перекрытием множества угроз?
8. Какими методами оценки экономической эффективности системы защиты объекта информатизации можно дополнить анализ трехдольного графа?
9. Как осуществляется декомпозиция общей задачи оценки эффективности функционирования системы защиты? Приведите пример модели элементарной защиты объекта информатизации и расчета прочности оболочки защиты.
10. Приведите пример модели многозвенной защиты объекта информатизации. Как в этом случае рассчитывается прочность защиты?

2. АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ МЕТОДИКИ COBIT

Цель практической работы: изучение методики и программного инструментария для анализа и оценки рисков информационной безопасности на примере методики COBIT и программного инструментария Coras.

Для выполнения практической работы на компьютере необходимо запустить программу из папки: *Исполняемые модули/2_Анализ рисков информационной безопасности*.

2.1. Описание методики COBIT для анализа рисков информационной безопасности

Терминология COBIT

Риски

Типы рисков — классификация рисков по источнику или их природе. Примером могут служить риски, связанные с нарушением законодательных актов, использованием той или иной технологии, нарушением бизнес-процессов.

Приемлемый уровень риска — его пороговое значение. Риски ниже приемлемого уровня или равные ему должны быть приняты руководством компании, а оставшиеся — минимизированы.

Стандарт управления рисками — схема, позволяющая определить, каким образом компания добивается снижения тех или иных рисков, какие механизмы при этом она использует, в каких случаях и как происходит принятие рисков или их снижение.

Матрица ИТ-рисков — таблица, представляющая собой картину рисков, «снимок» величин ИТ-рисков на момент проведения оценки.

Руководство рисками

Владелец процессов оценки рисков — ответственный за все процессы и мероприятия, из которых состоит управление рисками.

План работ по снижению рисков — методология управления рисками, содержащая правила разработки рекомендаций для снижения рисков, а собственно план должен включать в себя задачи по улучшению процессов оценки рисков.

Политики и процедуры — утвержденные корпоративные правила. Политики и процедуры определяют, каким образом должно осуществляться управление рисками на различных уровнях иерархии компании.

Обновление величин рисков — механизм, позволяющий на регулярной основе проводить оценку рисков и отслеживать их динамику, поскольку величины рисков постоянно находятся в движении, что может обеспечивать появление новых рисков.

Глобальный и системный уровни оценки ИТ-рисков — уровни, на которые методология оценки ИТ-рисков должна разделять свои задачи. Системный уровень — это уровень оборудования и операционной системы, базы данных, приложения, в то время как глобальный — это уровень организации процессов.

Резюме для руководителя — оповещение, которое должно быть включено в методологию управления ИТ-рисками и преследует цель донести до руководства своевременную и точную информацию для управления компанией.

Стратегия управления ИТ-рисками — методология управления рисками, предусматривающая способы управления рисками, например исключение (обход), снижение, принятие и страхование.

Идентификация

Определение компонентов риска — материальные и нематериальные активы, степень их защищенности, ценность, угрозы, потенциальный ущерб и вероятность реализации угроз.

Области рисков — бизнес-риски, нарушение законодательства, коммерческие, технологические и та область рисков, которая связана с человеческим фактором.

Обновление матрицы рисков — проведение компанией повторных оценок величин рисков на регулярной основе для принятия адекватных мер по управлению ИТ-рисками, поскольку последние обладают свойством меняться во времени по величине.

Меры оценки

Количественная оценка — величины рисков, выражающиеся в цифрах, например, в деньгах, времени простоя сервера, упущенной выгоде.

Качественная оценка — величины рисков, характеризующиеся относительно, например, риск «высокий», «средний», «низкий».

Способы управления

Независимое мнение — обращение компании к услугам третьих лиц для проверки эффективности некоторых процессов.

Возврат инвестиций — процедура, используемая руководством компании для оценки эффективности инвестиций.

Баланс способов управления — набор мер по снижению рисков, имеющий минимально возможную стоимость, которая достигается путем рационального сочетания предотвращающих, выявляющих, корректирующих и восстанавливающих способов управления.

Управление конфликтами — процесс выявления и решения возникающих время от времени конфликтов (например, сетевой экран может блокировать трафик Интернет-приложения).

Мониторинг

Мониторинг используемых способов управления — наблюдение за примененным способом управления с целью достижения его эффективности.

Процедура реагирования на инциденты — анализ происходящих событий и вынесение решений по этому поводу. Инциденты могут представлять собой негативные или позитивные события, например, действия хакера, обнаруженные одним из способов управления, могут дать столько же полезной информации для составления плана по минимизации рисков, сколько и успешное проникновение злоумышленника.

Согласование плана работ по снижению рисков — своевременное устранение обнаруженных недостатков в плане работ по минимизации рисков. Согласование необходимо, чтобы достичь уверенности в том, что план включает только правильные мероприятия.

Анализ рисков, как составляющая аудита информационной безопасности

Целью анализа рисков, связанных с эксплуатацией информационных систем (ИС), является оценка угроз (т.е. условий и факторов, которые могут стать причиной нарушения целостности системы, ее конфиденциальности, а также облегчить несанкционированный

доступ к ней) и уязвимостей (слабых мест в защите, которые делают возможной реализацию угрозы), а также определение комплекса контрмер, обеспечивающего достаточный уровень защищенности ИС. При оценивании рисков учитываются многие факторы: ценность ресурсов, значимость угроз, уязвимостей, эффективность имеющихся и планируемых средств защиты и многое другое.

Процесс управления направлен на определение событий, которые могут оказать влияние на организацию, и на управление связанным с этими событиями риском. При этом обеспечивается контроль над допустимым уровнем риска при разумной гарантии достижения целей организации. Управление рисками организации представляет собой непрерывный процесс, охватывающий всю организацию, осуществляется сотрудниками на всех уровнях организации (советом директоров, менеджерами и другими сотрудниками), используется при разработке и формировании стратегии, применяется во всей организации, на каждом ее уровне и в каждом подразделении и включает анализ портфеля рисков на уровне организации.

К мерам по управлению ИТ-рисками относятся: разработка нормативных документов; обеспечение физической безопасности и безопасности ИС; разграничение доступа к ресурсам компании; контроль состояния корпоративной ИС. Во-первых, определяется объект защиты — проводится инвентаризация информационных активов, оценивается их критичность для бизнес-процессов компании. Во-вторых, решается, от чего осуществляется защита. Для этого анализируются присущие системе уязвимости, определяется степень их критичности — вероятность того, что они могут быть реализованы.

Далее внедряются контрмеры, анализируется их результативность и принимается решение — оптимизировать или оставлять работать. Необходимо отслеживать изменения, происходящие как в ИС, так и в окружающей среде, чтобы своевременно вносить соответствующие коррективы.

Применение дополнительных мер по защите, позволяющих обеспечить приемлемую для организации величину риска (например, защитить и/или ограничить доступ в Интернет), дает возможность минимизировать или предупредить возможные риски.

Возможная последовательность шагов по предупреждению и минимизации рисков:

1) на этапе создания корпоративного стандарта управления рисками разрабатывается стандарт, который устанавливает процедуры по управлению рисками;

2) на этапе оценки рисков выполняются процедуры выявления факторов рисков и оценки их значимости, по сути — анализ вероятности того, что произойдут определенные нежелательные события, которые отрицательно повлияют на достижение целей проекта. Оценка рисков включает их идентификацию, анализ, оценку, а также методы снижения рисков или уменьшения связанных с ними неблагоприятных последствий;

3) назначается лицо, ответственное за все процессы и мероприятия по управлению рисками. В большинстве организаций это владелец активов, руководство компании;

4) этап обработки рисков предполагает использование одной из следующих стратегий: избежать, передать (страхование, аутсорсинг), минимизировать, принять;

5) в процессе мониторинга, идентификации и переоценки рисков для каждого из них следует определить и документировать события, которые можно отслеживать для того, чтобы понять, удалось ли избежать наступления риска, либо минимизировать последствия наступившего риска. Для каждого риска должны быть выполнены все действия, предусмотренные планом смягчения последствий риска;

6) этап совершенствования методологии и оценки остаточных рисков предполагает реагирование на инциденты с последующим анализом происходящих событий.

Несмотря на повышение интереса к управлению рисками используемые в настоящее время методики относительно неэффективны, поскольку этот процесс во многих компаниях осуществляется каждым подразделением независимо. Централизованный контроль (или надзор) над их действиями зачастую отсутствует, что исключает возможность реализации единого и целостного подхода к управлению рисками во всей организации.

В настоящее время используются два варианта подхода к анализу рисков — *базовый* и *полный*. Выбор зависит от оценки собственниками ценности своих информационных ресурсов и возможных последствий нарушения режима информационной безопасности. В простейшем случае собственники информационных ресурсов могут не оценивать эти параметры. Подразумевается, что ценность ресурсов с точки зрения организации не является чрезмерно высокой. В этом случае анализ рисков производится по упрощенной схеме: рассматривается стандартный набор наиболее распространенных угроз без оценки их вероятности и обеспечивается минимальный или базовый уровень информационной безопасности.

Полный вариант анализа рисков применяется в случае повышенных требований к информационной безопасности. В отличие от базового варианта, в том или ином виде оцениваются ресурсы, характеристики рисков и уязвимостей. Как правило, проводится анализ соотношения стоимость/эффективность нескольких вариантов защиты.

Таким образом, при проведении полного анализа рисков необходимо:

- определить ценность ресурсов;
- добавить к стандартному набору список угроз, актуальных для исследуемой ИС;
- оценить вероятность угроз;
- определить уязвимость ресурсов;
- предложить решение, обеспечивающее необходимый уровень информационной безопасности.

В ИС с повышенными требованиями к информационной безопасности при выполнении полного анализа рисков приходится решать ряд сложных проблем, заключающихся в том, как определить ценность ресурсов, как составить полный список угроз и оценить их параметры, как правильно выбрать эффективные контрмеры.

Риск характеризует опасность, которой может подвергаться система и использующая ее организация.

Степень риска зависит от ряда факторов:

– ценности ресурсов;
– вероятности реализации угроз;
– простоты использования уязвимости для реализации угроз;
– существующих или планируемых к внедрению средств обеспечения информационной безопасности, которые уменьшают число уязвимостей, вероятность возникновения угроз и возможность негативных воздействий.

Определение ценности ресурсов

Ресурсы обычно подразделяются на несколько классов.

Пример классификации ресурсов и стоимостная их оценка приведены на рис. 2.1.

Для каждого класса необходима своя методика определения ценности элементов, помогающая выбрать подходящий набор критериев. Эти критерии служат для описания потенциального ущерба,

Рис. 2.1. Классификация и определение ценности ресурсов

связанного с нарушением конфиденциальности и целостности ИС, уровня ее доступности.

Физические ресурсы оцениваются по стоимости их замены или восстановления их работоспособности. Качественные оценки стоимостных величин затем преобразуются в ранговую шкалу, которая может использоваться также и для оценок информационных ресурсов. Программные ресурсы оцениваются тем же способом, что и физические, на основе определения затрат на их приобретение или восстановление.

Кроме критериев, учитывающих финансовые потери, коммерческие организации могут применять критерии, отражающие:

– ущерб репутации организации;
– неприятности, связанные с нарушением действующего законодательства;
– ущерб для здоровья персонала;
– ущерб, связанный с разглашением персональных данных отдельных лиц;
– финансовые потери от разглашения информации;
– финансовые потери, связанные с восстановлением ресурсов;
– потери, связанные с невозможностью выполнения обязательств;
– ущерб от дезорганизации деятельности.

Очевидно, что процесс оценивания потерь по приведенным критериям часто носит субъективный характер.

Могут использоваться и другие критерии в зависимости от основной деятельности организации.

Оценка характеристик факторов риска

Ресурсы должны быть проанализированы по величине оценки воздействия возможных атак (спланированных действий внутренних или внешних злоумышленников) и различных нежелательных событий естественного происхождения. Кроме того, необходимо идентифицировать уязвимости — слабые места в системе защиты, которые делают возможной реализацию угроз.

Вероятность угрозы повышается при наличии следующих факторов:

– привлекательность ресурса (этот показатель учитывается при рассмотрении угрозы умышленного происхождения);
– возможность использования ресурса для получения дохода (показатель учитывается при рассмотрении угрозы умышленного происхождения);
– простота использования уязвимости при проведении атаки.

Технология анализа рисков

Существует множество методик анализа рисков. Некоторые из них основаны на достаточно простых табличных методах и не предполагают применения специализированного программного инструментария, другие, наоборот, его используют.

В табличных методах можно наглядно отразить связь факторов негативного воздействия (показателей ресурсов) и вероятностей реализации угроз с учетом показателей уязвимостей.

Подобные методы сводятся к нескольким несложным шагам. Вот пример одного из таких методов.

На первом шаге оценивается негативное воздействие (показатель ресурса) по заранее определенной шкале (скажем, от 1 до 5) для каждого ресурса, которому угрожает опасность.

На втором шаге по той же шкале оценивается вероятность реализации каждой угрозы.

На третьем шаге вычисляется показатель риска. В простейшем варианте методики это делается путем умножения. Однако необхо-

димо помнить, что операция умножения определена для количественных шкал.

На четвертом шаге угрозы ранжируются по значениям их фактора риска.

В настоящее время на рынке существует около двух десятков программных продуктов для анализа рисков: от простейших, ориентированных на базовый уровень безопасности, до сложных и дорогостоящих, позволяющих реализовать полный вариант анализа рисков и выбрать комплекс контрмер требуемой эффективности.

Программные средства, необходимые для полного анализа рисков, строятся с использованием структурных методов системного анализа и проектирования (*Structured Systems Analysis and Design*, SSADM) и представляют собой инструментарий для выполнения следующих операций:

– построение модели ИС с позиции информационной безопасности;
– оценка ценности ресурсов;
– составление списка угроз и уязвимостей, оценка их характеристик;
– выбор контрмер и анализа их эффективности;
– анализ вариантов построения защиты;
– документирование (генерация отчетов).

Примерами программных продуктов этого класса являются CRAMM (разработчик — компания *Logica*, Великобритания), MARION (разработчик *CLUSIF,* Франция), *Risk Watch* (США).

Обязательным элементом этих продуктов является база данных, содержащая информацию по инцидентам в области информационной безопасности, позволяющая оценить риски и уязвимости, эффективность различных вариантов контрмер в определенной ситуации.

2.2. Порядок работы с программным инструментарием CORAS для анализа рисков информационной безопасности

Программный пакет Coras предназначен для анализа рисков безопасности. Программное обеспечение использует язык UML (сокр. от англ. *Unified Modeling Language* — унифицированный язык моделирования) — язык графического описания для объектного моде-

лирования в области разработки программного обеспечения. UML является языком широкого профиля, это открытый стандарт, использующий графические обозначения для создания абстрактной модели системы, называемой UML-моделью. UML был создан в основном для определения, визуализации, проектирования и документирования программных систем.

В программном обеспечении используются элементы, перечень которых представлен в табл. 2.1.

Таблица 2.1

Элементы программы

Вид	*Название на английском языке*	*Название на русском языке*
	Asset	Ценность, информация, подлежащая защите
	Stakeholder	Владелец информации
	Threat Human Accidental	Угроза непреднамеренная, связанная с человеческим фактором воздействия
	Threat Human Deliberate	Угроза преднамеренная, связанная с человеческим фактором воздействия
	Threat Non Human	Угроза, не связанная с человеческим фактором воздействия
	Threat Scenario	Сценарий угрозы
	Vulnerability	Уязвимость
	Unwanted Incident	Нежелательный инцидент
	Risk	Риск
	Treatment	Противодействие угрозе

На рис. 2.2. представлено главное окно программы, на рис. 2.3–2.6 — окна более низких уровней.

Окно программы можно разделить на следующие зоны: меню (*1*), панель инструментов (*2*), области проводника (*3*) и построения диаграммы (*4*).

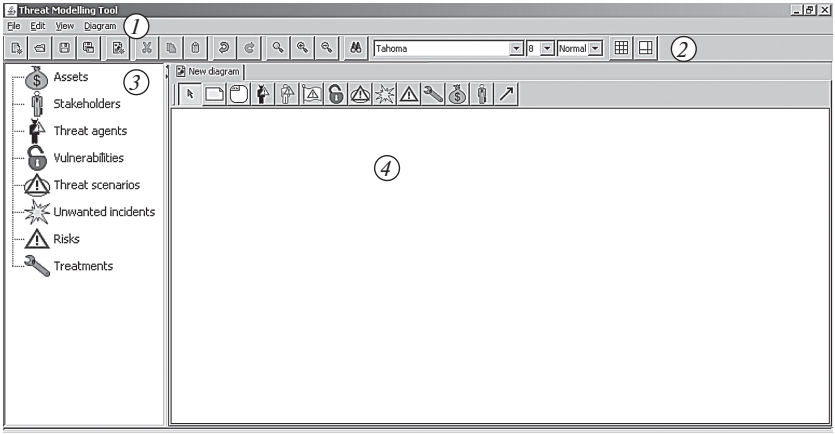


Рис. 2.2. Главное окно программы

Меню, расположенное вверху, имеет все стандартные команды:

1) File/Файл

1. Создать
2. Открыть
3. Сохранить
4. Сохранить как
5. Новая диаграмма
6. Экспорт в:
   6.1. Png
   6.2. Jpg
   6.3. Svg
7. Выход

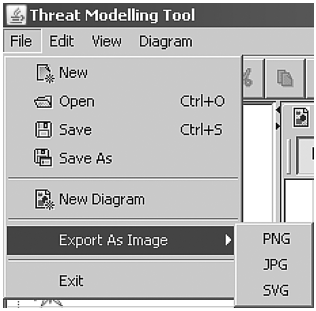


Рис. 2.3. Подменю Файл

2) Edit/Редактирование

1. Удалить
2. Копировать
3. Вставить
4. Отменить
5. Повторить

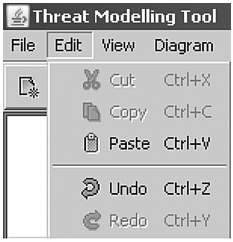


Рис. 2.4. Подменю Редактирование

3) View/Вид

1. Масштаб 100%
2. Приблизить
3. Отдалить

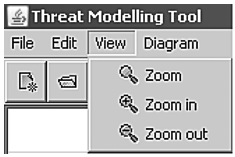


Рис. 2.5. Подменю Вид

4) Diagram/Диаграмма

1. Ориентация
   1.1. Альбомная
   1.2. Книжная

Рис. 2.6. Подменю Диаграмма

Панель инструментов представлена на рис. 2.7–2.10.

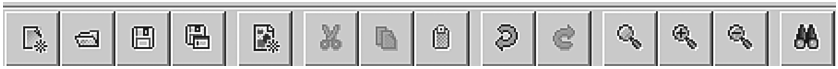


Рис. 2.7. Кнопки главного меню и поиска

Первая половина кнопок, расположенных на панели — дублирование действий главного меню. Далее расположена кнопка, реализующая поиск.

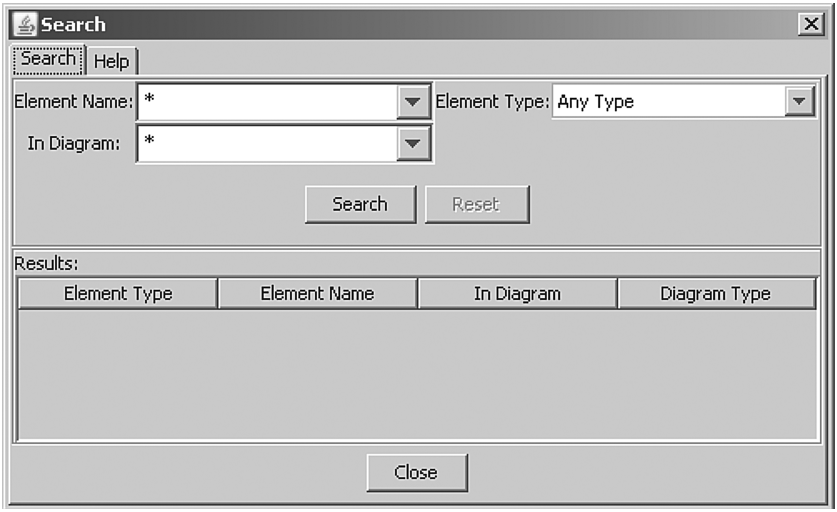


Рис. 2.8. Окно поиска

Поиск элемента осуществляется по его имени и типу. Также можно указать имя диаграммы. После нажатия на кнопку Search (Искать), в таблице, расположенной под введенными данными для поиска, отобразятся подходящие записи.

Шапка таблицы — условия поиска: тип элемента, его имя, название диаграммы, ее тип.

После того как поиск завершен, кнопка Reset (Сброс) становится активной. Нажатие на нее сбросит все введенные и найденные данные.

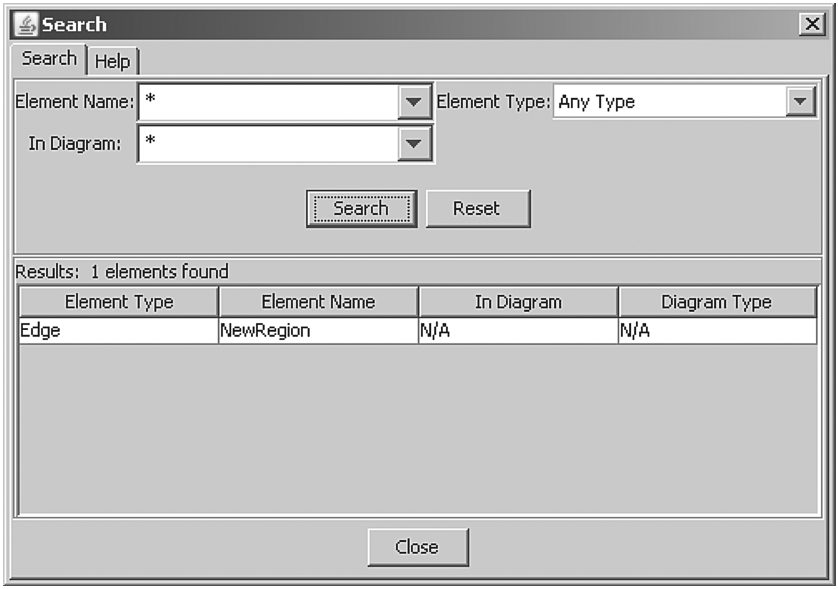


Рис. 2.9. Результаты поиска

На панели редактирования шрифта для пользователя реализована возможность изменения шрифта, его размера и выделение: обычный (Normal), жирный (Bold), курсив (Italic).

Две последние кнопки, расположенные на панели инструментов (см. рис. 2.10), позволяют добавлять сетку на область построения диаграмм, а также отметить лист размером А4.

Рис. 2.10. Редактирование шрифта и страницы

Слева расположены все объекты, используемые в данной модели угроз для анализа рисков информационной безопасности. При добавлении на лист моделирования какого-либо объекта он сразу отображается в этой схеме, представленной в виде дерева, что удобно для понимания связей, которые были установлены между объектами (см. рис. 2.11).

Проводник скрывается и отображается посредством нажатия на стрелки, нанесенные на границу между областью построения диаграммы и самим проводником (рис. 2.12).

При создании новой диаграммы (File/New или кнопка New на панели инструментов) на области построения диаграмм появляется новая вкладка с именем по умолчанию New diagram.

Для изменения имени диаграммы необходимо щелкнуть правой кнопкой мыши на заголовке вкладки и

Рис. 2.11. Проводник объектов, используемых в диаграмме

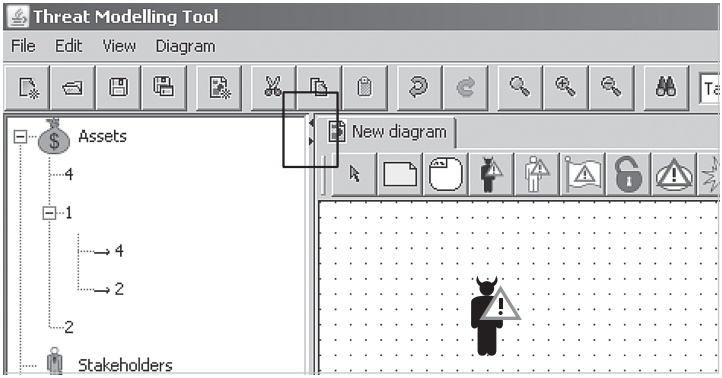


Рис. 2.12. Скрыть/отобразить проводник

выбрать Edit diagram name. В появившемся диалоговом окне ввести имя (рис. 2.13–2.14).

Для удаления диаграммы следует выбрать Delete diagram.

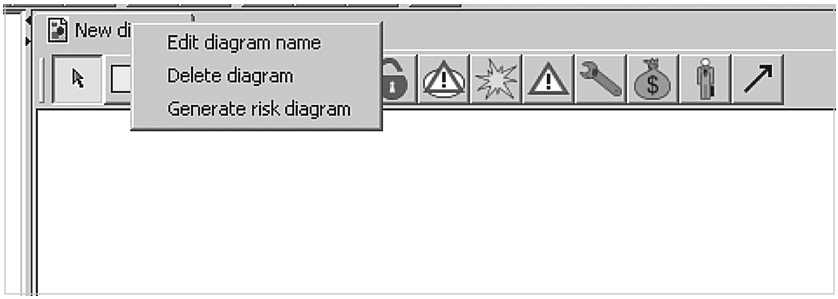


Рис. 2.13. Вкладка для работы с диаграммой

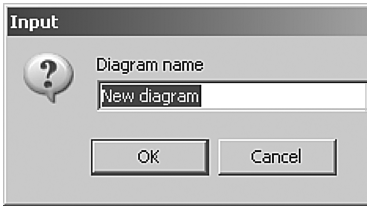


Рис. 2.14. Изменение имени диаграммы

Generate risk diagram генерирует картину рисков для данного проекта.

Панель объектов, которые непосредственно используются при моделировании, расположена на вкладке диаграммы (рис. 2.15).

Кроме перечисленных в табл. 2.1 объектов, на этой панели инструментов есть кнопка примечания (*comment*) для добавления подписей, разъяснений, область (*region*) для выделения объектов в отдельные области (например, в пределах охраняемой территории и за ее пределами). Первая стрелка служит для выделения, перемещения объектов, последняя (рис. 2.15) — для установления связей между объектами. Чтобы установить связь, необходимо выполнить следующие действия:

Рис. 2.15. Панель объектов

1) выбрать последнюю кнопку (стрелка) на панели инструментов диаграммы (см. рис. 2.15);

2) навести на объект, являющийся началом связи и нажать левую кнопку мыши;

3) объект начинает выделяться синим цветом;

4) не отпуская кнопки мыши, перевести ее на объект, являющийся окончанием связи;

5) после того как начальный объект прекратит выделяться, будет выделен конечный, а после окончания выделения установится связь между объектами.

Установление связей необходимо для создания модели рисков.

Для того чтобы изменить имя объекта, нужно выбрать его и щелкнуть мышью — появится строка для ввода.

Методология анализа рисков информационной безопасности CORAS включает семь этапов.

1) Вводная встреча. Целью этого этапа является полное понимание того, что подлежит анализу. Во время этой встречи аналитики собирают информацию, основанную на представлениях заказчика.

2) Отдельная встреча с представителями заказчика. Аналитики знакомят со своим пониманием проблемы на основании полученных на первом этапе информации и документов, к которым заказчик открыл доступ для аналитиков. На этом этапе идентифицируются базовые угрозы, уязвимости, сценарии угроз и нежелательные инциденты.

3) Третий этап включает более подробное описание той ситуации, которую необходимо проанализировать с учетом всех предложений и предварительных условий. Он заканчивается, как только вся информация будет одобрена заказчиком.

4) Четвертый этап включает в себя идентификацию всех потенциально возможных нежелательных инцидентов, а также угроз и уязвимостей.

5) На пятом этапе оцениваются последствия осуществления нежелательных инцидентов, а также вероятность этих инцидентов.

6) На шестом этапе формируется полная картина рисков, которая далее редактируется с учетом дополнительной информации.

7) На седьмом этапе формируется обоснование и описание действий, необходимых для повышения эффективности системы защиты.

2.3. Задания для анализа рисков информационной безопасности с использованием программного пакета Coras

1. Описать структуру предприятия (варианты заданий см. Приложение 1).

2. Составить перечень объектов защиты на рассматриваемом предприятии.

3. Определить и описать полное множество угроз информационной безопасности на предложенном к анализу предприятии.

4. С использованием программного пакета Coras построить диаграмму активов; таблицу и матрицу рисков; модели угроз; диаграмму рисков с характеристикой последствий осуществления угрозы; диаграмму угроз после добавления противодействий.

5. Сформулировать выводы на основании анализа диаграммы неприемлемых рисков об эффективности системы защиты рассматриваемого предприятия и предложить мероприятия по снижению рисков информационной безопасности.

6. В отчете по практической работе должны быть представлены:
- схема и описание организации в соответствии с полученным вариантом;
- таблица с перечнем угроз безопасности;
- таблица с перечнем объектов защиты;
- диаграммы, перечисленные в п. 4;
- выводы по результатам анализа диаграммы неприемлемых рисков.

Пример отчета приведен в Приложении 2.

Контрольные вопросы и задания

1. Какая информация должна быть собрана на объекте оценки для проведения анализа информационных рисков?
2. В каких единицах измеряется риск?
3. Выберите оптимальную стратегию управления рисками в следующем случае: веб-сервер компании находится внутри корпоративной сети и его программное обеспечение, возможно, содержит уязвимости.
4. Какую информацию необходимо получить на объекте оценки для определения ущерба по угрозе <*нарушение целостности информации*>?

5. Какую информацию необходимо получить на объекте оценки для определения ущерба по угрозе <*нарушение конфиденциальности информации*>?
6. В случае анализа рисков ИС на базовом уровне какими стандартами в области защиты информации необходимо руководствоваться?
7. В случае полного анализа рисков ИС какие подходы обычно используются на практике?
8. Какие этапы должен включать аудит информационной безопасности?
9. Как осуществляется анализ информационных рисков, угрозы и уязвимости системы по двум факторам?
10. Как осуществляется анализ информационных рисков, угрозы и уязвимости системы по трем факторам?

3. СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ ПАРЕТО-ОПТИМАЛЬНЫХ РЕШЕНИЙ В ОБЛАСТИ ПРОЕКТИРОВАНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

Цель практической работы: изучение возможностей использования систем поддержки принятия решений при проведении оценки эффективности альтернативных проектов системы защиты информации на примере метода парето-оптимального оценивания.

Для выполнения практической работы на компьютере необходимо запустить программу из папки: *Исполняемые модули/3_СППР на основе критериев парето-оптимальности*.

3.1. Описание метода принятия решений в разработке системы защиты информации на основе закона Парето и метода достижимых целей

Разработка системы защиты информации с позиций теории принятия решений классифицируется по способу отображения как слабоструктурированная или смешанная проблема, поскольку содержит как качественные, так и количественные элементы, причем качественные, малоизвестные и неопределенные стороны имеют тенденцию к доминированию.

Под термином «принятие решений» подразумевается действие над множеством альтернатив (систем, ситуаций, факторов и т.д.), в результате которого получается подмножество выбранных альтернатив.

Постановка задачи и применение методов принятия решений зависят от многих факторов:

- множество альтернатив может быть конечным или бесконечным;
- оценка может осуществляться по одному или нескольким критериям, которые могут иметь как количественный, так и качественный характер;
- алгоритм выбора может быть однократным или адаптивным и повторяющимся;

- последствия выбора могут быть точно известны или носить вероятностный характер.

Решение задачи в рамках теории принятия решений начинается с генерации множества альтернатив. Затем альтернативы необходимо структурировать, с этой целью выделяют критерии оценки альтернатив, характеризующие эти альтернативы количественно или качественно. Количественные критерии описывают свойства альтернатив численно, например, критерий стоимости. Качественные критерии описывают неколичественные свойства альтернатив, например, цвет (черный, белый), или количественные свойства, которые трудно оценить точно, например, риск (низкий, средний, высокий). Для того чтобы можно было применять расчеты и производить действия над качественными критериями им ставится в соответствие некая шкала, которая кодирует значения критерия, например цвет (0 — черный, 1 — белый).

При оценивании систем, в частности, информационных, выделяют две группы критериев:

– критерии качества систем;
– критерии эффективности систем.

Критерии качества обозначают свойство или совокупность существенных свойств системы, обуславливающих ее пригодность к целевому использованию. При оценивании качества системы признается целесообразным введение нескольких уровней качества. Рассмотрим их в порядке иерархической значимости.

- *Устойчивость* — способность системы сохранять свою работоспособность после отказа одного или нескольких компонентов системы, определяемая как число любых последовательных единичных отказов компонентов системы, после которого сохраняется работоспособность системы в целом.
- *Помехоустойчивость* — способность системы без искажений воспринимать, передавать и обрабатывать информационные потоки при наличии возмущения, воздействующего на систему. Помехоустойчивость характеризуется такими показателями как надежность систем связи; пропускная способность; возможность эффективного кодирования/декодирования; электромагнитная совместимость электронных средств и т.д.
- *Управляемость* — способность системы переходить за конечное время в требуемое состояние под влиянием управляющих воздействий. Управляемость включает такие понятия как гибкость

управления системой; оперативность; точность; производительность; инерционность и т.д.

- *Способность* — это качество системы, определяющее ее возможности по достижению требуемого результата на основе имеющихся ресурсов в заданный период времени. Иными словами, способность — это потенциальная эффективность функционирования системы, способность получить требуемый результат при идеальном способе использования ресурсов и в отсутствие воздействий внешней среды.
- *Самоорганизация* является наиболее сложным качеством системы. Самоорганизующаяся система способна изменять свою структуру, параметры, алгоритмы функционирования для повышения эффективности. Принципиально важными свойствами этого уровня являются свобода выбора решений, адаптируемость, самообучаемость и способность к распознаванию ситуаций.

При исследовании качества системы для простых систем часто ограничиваются исследованием одного критерия, например, устойчивости. Для сложных систем, какими являются средства защиты информации (СЗИ), выбор критериев качества зависит от сложности системы; целей исследования; наличия информации; условий применения системы.

Критерии эффективности систем соответствуют комплексному операционному свойству процесса функционирования системы, характеризующему его приспособленность к достижению цели операции (выполнению задачи системы).

К этим критериям относятся следующие:

- *результативность операций*, которая обусловливается получаемым целевым эффектом, ради которого функционирует система;
- *ресурсоемкость*, характеризующаяся наличием ресурсов всех видов, используемых для получения целевого эффекта;
- *оперативность*, характеризующаяся расходом времени, потребного для достижения цели;

В совокупности результативность, ресурсоемкость и оперативность порождают комплексное свойство системы — эффективность как степень приспособленности системы к достижению цели.

После того как было сформировано множество альтернатив и множество критериев, необходимо выбрать метод (алгоритм) реше-

ния. Одним из наиболее распространенных методов принятия решений в задаче разработки СЗИ является метод экспертной оценки, так как при исследовании сложных ИС (в том числе СЗИ), при генерировании альтернатив наиболее часто прибегают к услугам экспертов — лиц, обладающих достаточным опытом и знаниями в рассматриваемой предметной области. К тому же аппарат обработки экспертных мнений достаточно хорошо проработан и используется во многих практических областях.

Организация работы экспертов включает следующие основные этапы:

- формулировка цели экспертного опроса;
- создание рабочей группы;
- разработка сценария проведения сбора информации и выбор методов обработки мнений;
- подбор экспертов в соответствии с целями опроса;
- проведение сбора экспертной информации;
- анализ экспертной информации;
- интерпретация полученных результатов и подготовка заключения для лица, принимающего решение.

Методы обработки мнений экспертов позволяют структурировать множество альтернатив при различных суждениях экспертов. Для этого при формировании набора критериев нужно учитывать мнение каждого эксперта, а затем объединить это множество в одно. Для оценки сравнительной значимости критериев используется компромиссное ранжирование: каждый эксперт дает свое ранжирование критериев по важности, и на основе индивидуального ранжирования строится, например, *обобщенная матрица сравнений с использованием строчных сумм*, а сам способ такого ранжирования называется *методом строчных сумм*.

Теория принятия решений в условиях риска и неопределенности основывается на следующих исходных положениях.

Объект принятия решения четко детерминирован и по нему известны основные из возможных факторов риска. В финансовом менеджменте такими объектами выступают отдельная финансовая операция, конкретный вид ценных бумаг, группа взаимоисключающих реальных инвестиционных проектов и т.п.

По объекту принятия решения избран показатель, который наилучшим образом характеризует эффективность этого решения. По крат-

косрочным финансовым операциям таким показателем избирается обычно сумма или уровень чистой прибыли, а по долгосрочным — чистый приведенный доход или внутренняя норма доходности.

По объекту принятия решения избран показатель, характеризующий уровень его риска. Финансовый риски характеризуются обычно степенью возможного отклонения ожидаемого показателя эффективности (чистой прибыли, чистого приведенного дохода и т.п.) от средней или ожидаемой его величины.

Имеется конечное число альтернатив принятия решения (конечное число альтернативных реальных инвестиционных проектов, конкретных ценных бумаг, способов осуществления определенной финансовой операции и т.п.).

Имеется конечное число ситуаций развития события под влиянием изменения факторов риска. В финансовом менеджменте каждая из таких ситуаций характеризует одно из возможных предстоящих состояний внешней финансовой среды под влиянием изменений отдельных факторов риска. Число таких ситуаций в процессе принятия решений должно быть детерминировано в диапазоне от крайне благоприятных (наиболее оптимистическая ситуация) до крайне неблагоприятных (наиболее пессимистическая ситуация).

По каждому сочетанию альтернатив принятия решений и ситуаций развития события может быть определен конечный показатель эффективности решения (конкретное значение суммы чистой прибыли, чистого приведенного дохода и т.п., соответствующее данному сочетанию).

Как было указано ранее, эксперты оценивают альтернативные проекты по созданию СЗИ на предприятии по указанным ранее критериям. Однако данная система оценки должна еще включать и экономические показатели, такие как стоимость, затраты на эксплуатацию, амортизация и прочие.

Логично предположить, что если исходить только из критериев эффективности и качества, то правильный выбор будет за той системой, которая достигнет максимальных показателей по двум группам критериев. Однако такая СЗИ может быть неэффективна в отношении финансовых затрат на ее реализацию, которые не были учтены первоначально при оценке альтернатив. В действительности приходится исходить из того, что ресурсы и возможности любой компании ограничены, и существует необходимость выбирать не лучшие или

худшие системы, а оптимальные по ряду ключевых критериев, о которых договариваются эксперты, участвующие в оценке. Такой выбор всегда будет сопровождаться дискуссиями по поводу того, какую систему можно будет назвать оптимальной и почему. Более того, разные участники могут преследовать разные цели, например, специалист по защите информации будет стремиться выбрать наиболее надежную и безопасную СЗИ, пользователи же желают, чтобы такая система была удобной и простой в работе, бухгалтер — к тому, чтобы она была наименее затратной в эксплуатации и недорогой при покупке. Таким образом, среди участников таких переговоров нужно достигнуть компромисса в ситуации, когда мнения и желания участников будут учтены и путем оправданных целесообразных уступок можно будет достигнуть оптимального соотношения рассматриваемых критериев и выбрать альтернативу, которая устроит их всех. Для того чтобы эти дискуссии были конструктивны и помогали вырабатывать единую концепцию, необходимо обеспечить всех участников подробным описанием альтернатив с их оценкой по указанным критериям, включая экономические. Далее необходимо оценить, как эти критерии взаимодействуют между собой. С этой позиции возможно рассмотреть закон Парето и принцип оптимизации по Парето.

Закон Парето, или принцип 20/80 — эмпирическое правило, получившее свое название в честь экономиста и социолога Вильфредо Парето (*Vilfredo Pareto*, 1848–1923), в наиболее общем виде формулируется как «20% усилий дают 80% результата, а остальные 80% усилий — лишь 20% результата». Принцип 20/80 может использоваться как базовая установка в анализе факторов эффективности какой-либо деятельности и оптимизации ее результатов: правильно выбрав минимум самых важных действий, можно быстро получить значительную часть от планируемого полного результата, при этом дальнейшие улучшения неэффективны и могут быть неоправданными (согласно кривой Парето).

Следствия из закона Парето формулируются следующим образом.

1. Большая часть усилий не дает желаемых результатов.

2. То, что мы видим, не всегда соответствует действительности — всегда имеются скрытые факторы.

3. То, что мы рассчитываем получить в результате, как правило, отличается от того, что мы получаем, — всегда действуют скрытые силы.

4. Обычно слишком сложно и утомительно разбираться в том, что происходит, а часто это и не нужно: необходимо лишь знать — работает ли ваша идея, и изменять ее так, чтобы она заработала, а затем поддерживать ситуацию до тех пор, пока идея не перестанет работать.

5. Большинство удачных событий обусловлено действием небольшого числа высокопроизводительных сил; большинство неприятностей связано с действием небольшого числа высокодеструктивных сил.

6. Большая часть действий, групповых или индивидуальных, являет собой пустую трату времени.

Математический анализ закона Парето позволяет высказать в его отношении две основные претензии:

- в качественной формулировке (т.е. без учета конкретных значений 20/80) закон представляет собой тривиальное с позиций математики наблюдение, согласно которому в ситуации, когда результат складывается из действия множества различных факторов, вклад этих факторов в результат часто бывает различным;
- количественная часть закона математически очевидно некорректна:

  1) действительное распределение вклада большей и меньшей частей факторов в реальной жизни бывает каким угодно, и вовсе не обязательно оно равно 20/80;

  2) легко проверить, что конкретные значения распределения меняются даже при анализе одних и тех же данных, достаточно изменить правила группировки выборочных значений;

  3) можно также заметить, что основное следствие закона Парето, на котором базируется все его применение — то, что факторов, дающих наибольший вклад в результат, всегда немного, — является лишь эмпирическим наблюдением, которое вовсе не обязано сбываться в каждом конкретном случае.

Указанные факты определяют границы применимости закона Парето: он ни в коем случае не должен рассматриваться как непреложный закон природы с конкретно заданными числовыми параметрами. Применение же его в качестве общего принципа, требующего обращать внимание на неравномерность вклада разных факторов в результат и необходимость уделять различное внимание разным по важности факторам, вполне оправдано и полезно.

В применении принципа Парето есть еще один «подводный камень»: в реально существующих системах такие свойства как полнота, качество, функциональность описываются не одним параметром, а некоторой их совокупностью. Даже если распределение вклада различных факторов в каждый из этих параметров по отдельности определяется законом Парето, как правило, вклады одного и того же фактора в различные параметры системы неодинаковы. Один и тот же фактор для одного параметра может относиться к числу малозначительных, для другого — попасть в число определяющих. Поэтому, пытаясь оптимизировать что-либо путем избавления от ненужных частей, оптимизатор должен быть уверен, что учитывает все существенные параметры системы.

Несмотря на критику, закон, описанный Парето, и выявленные им статистические закономерности используются в методах оптимизации, включая методы выбора оптимальных альтернатив.

Оптимальность по Парето — такое состояние системы, *при котором значение каждого частного показателя* (*критерия*), *характеризующего систему* (*принятия решений*), *не может быть улучшено без ухудшения других.*

Таким образом, по словам самого Парето: «Всякое изменение, которое никому не приносит убытков, а некоторым приносит пользу (по их собственной оценке), является улучшением». Значит, признается право на все изменения, которые не приносят никому дополнительного вреда и оптимальным решением принимается такое, которое является доминирующим.

Определение: альтернатива A называется доминирующей по отношению к альтернативе B, если по всем критериям оценки альтернативы A не хуже, чем альтернативы B, а хотя бы по одному критерию оценка A лучше. Альтернатива B при этом называется доминируемой.

Отношение Парето: $(y_i, y_j) \in R_p \rightarrow \forall k$: $[f_k(y_i) \geq f_k(y_j)] \wedge [f(y_i) \neq f(y_j)]$.

Если для некоторой точки $y^0 \in Y$ не существует более предпочтительной по Парето точки, т.е. такой точки y, что $(y, y^0) \in R_p$, то тогда точка y^0 называется эффективным, или *парето-оптимальным решением многокритериальной задачи*, *относится к множеству Парето* (рис. 3.1).

Альтернатива является парето-оптимальной, если она лучше других по какому-то из критериев.

Рис. 3.1. Парето-оптимальное множество

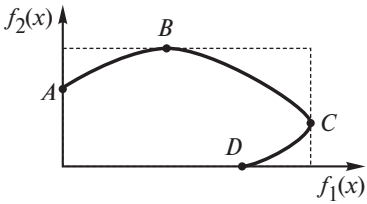


Рис. 3.2. Отношение Парето

Альтернативы, принадлежащие к множеству Парето, называются несравнимыми. Их невозможно сравнить непосредственно на основе критериальных оценок. Они не находятся в отношении доминирования.

Далее приводятся аксиомы, являющиеся основой принципа Парето.

- *Аксиома исключения доминирующих решений*: для всякой пары допустимых решений $x', x'' \in X$, для которых имеет место соотношение $x' \succ_X x''$, выполнено

$$x'' \notin C(X).$$

- *Аксиома Парето*: для всех пар допустимых решений $x', x'' \in X$, для которых имеет место неравенство $f(x') \geq f(x'')$, выполняется соотношение

$$x' \succ_X x'',$$

где $\succ_X$ — отношение предпочтения;

X — множество допустимых решений;

f — векторный критерий.

Принцип Парето: наилучшее решение многокритериальной задачи всегда выбирается из парето-оптимального множества.

Алгоритм нахождения множества Парето

1. Принять $P(Y) = Y$, $i = 1$, $j = 2$. Создается текущее множество парето-оптимальных векторов, которое в начале совпадает с множеством Y.

2. Проверить выполнение неравенства $y^{(i)} \geq y^{(j)}$. Если да, то перейти к п. 3. Если нет, то перейти к п. 5.

3. Удалить из текущего множества $P(Y)$ вектор $y^{(i)}$, так как он не является парето-оптимальным. Перейти к п. 4.

4. Проверить выполнение неравенства $j < N$. Если да, то положить $j = j + 1$ и вернуться к п. 2. Если нет, то перейти к п. 7.

5. Проверить выполнение неравенства $y^{(i)} \geq y^{(j)}$. Если да, то перейти к п. 6. Если нет, то перейти к п. 4.

6. Удалить из текущего множества $P(Y)$ вектор $y^{(i)}$, так как он не является парето-оптимальным. Перейти к п. 7.

7. Проверить выполнение неравенства $i < N - 1$. Если да, то положить $i = i + 1$, $j = j + 1$ и вернуться к п. 2. Если нет, закончить вычисления.

Таким образом, рассмотрев наиболее распространенные подходы к поиску оптимального решения многокритериальных задач, в том числе в условиях неопределенности, на практике именно метод парето-оптимальности будет наиболее удобным и эффективным, поскольку позволяет выделить ряд критериев, не вносящих существенный вклад в достижение оптимальной эффективности и выбрать оптимального решение.

Описанный закон Парето лежит в основе метода достижимых целей (МДЦ), который предлагается использовать. МДЦ позволяет разрабатывать модели систем (в том числе СЗИ), описывать их характеристики, задавать ограничения и визуализировать принятие оптимальных решений с помощью графиков замещения критериев. Парето-оптимизация позволяет найти такое состояние системы, при котором значение каждого частного показателя (критерия), характеризующего систему (принятия решений), не может быть улучшено без ухудшения других. Данный метод оперирует таким понятием как недоминируемые цели (или альтернативы). Дадим краткое толкование недоминируемой цели: альтернатива *A* называется доминирующей (или недоминируемой) по отношению к альтернативе *B*, если по всем критериям оценки альтернативы *A* не хуже, чем альтернативы *B*, а хотя бы по одному критерию оценка *A* лучше. Альтернатива *B* при этом называется доминируемой (или недоминирующей). Другими словами, при прочих одинаковых условиях альтернатива *A* лучше альтернативы *B*.

Данный метод также основывается на том, что оптимизировать можно лишь небольшую часть критериев, остальные же надо либо зафиксировать, либо наложить некие ограничения. Это основано на том, что среди всего множества критериев лишь небольшая часть вносит существенный вклад в качественные признаки системы соответственно одновременно оценивать все множество критериев затруднительно и бессмысленно с позиции закона Парето (20% критериев составляют 80% от всей оценки системы).

Итак, данный метод предполагает следующие шаги:

1) построение множества достижимых целей (альтернатив) в пространстве критериев (выбранных для оптимизации);

2) создание графиков, визуально отображающих кривые объективного замещения между различными парами критериев;

3) выбор оптимальной (компромиссной) цели;

4) расчет выбранной цели и выработка стратегии по внедрению выбранной СЗИ.

Рассмотрим данный метод более подробно на примере. Пусть существуют четыре альтернативных друг другу проекта СЗИ; обозначим их через x_1, x_2, x_3, x_4, причем $x_i > 0$ ($i = 1...4$), $\sum x_i = 1$. Пусть существует три критерия, которые мы выбрали для оценки, остальные были приняты как константы (или были наложены ограничения). $y_1 = a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4$ — критерий общей стоимости СЗИ, a_i — стоимость i-альтернативы. $y_2 = \beta_1x_1 + \beta_2x_2 + \beta_3x_3 + \beta_4x_4 + \beta_0(1-x_1-x_2-x_3-x_4)$ — критерий риска, оставшегося после внедрения СЗИ, где β_0 — риск до внедрения СЗИ; β_i — остаточный риск i-й альтернативы; $y_3 = g_1x_1 + g_2x_2 + g_3x_3 + g_4x_4$ — критерий надежности. Рассмотрим альтернативы, оценив их по критериям y_1 и y_2. Пусть заданы такие значения коэффициентов, что в результате получается следующий график (рис. 3.3).

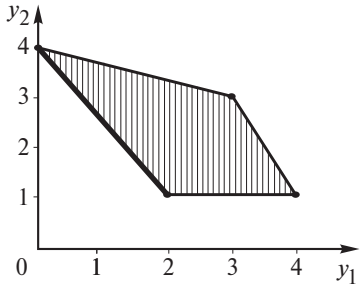


Рис. 3.3. Кривая объективного замещения стоимости и остаточных рисков

Поскольку оба параметра необходимо уменьшить (стоимость и риски), то юго-западная граница области содержит подмножество парето-оптимальных решений. К этой области принадлежит одна единственная точка с координатами (2, 1). Она является парето-оптимальной, потому что при одном и том же уровне риска ее стоимость меньше чем у точки (4, 1), иначе говоря, увеличение стоимости после точки (2, 1) не приводит к значительному снижению рисков, значит решение (4, 1) неоптимально. Кривая объективного замещения показывает, сколько придется платить за уменьшение выброса загрязнителя, если используются эффективные (т.е. разумные) решения, в МДЦ также означает множество парето-оптимальных решений или недоминируемое множество (на рис. 3.3 линия, выделенная жирным).

МДЦ позволяет создавать огромное множество таких парных критериальных графиков (общее число оценивается сверху как $C_n^2 = \dfrac{n!}{2\cdot(n-2)!}$), однако для каждого такого графика будет иметься своя

область эджварто-парето (ОЭП или недоминируемое множество), причем эти множества для каждой пары критериев не обязательно должны пересекаться. Потому если необходимо найти решения оптимальные сразу по нескольким показателям (трем и более), то надо располагать альтернативы в трехмерном (*n*-мерном) пространстве отобранных критериев (рис. 3.4).

Однако анализировать трехмерные пространства с целью поиска областей оптимальных решений трудно, поэтому предлагается использовать серию рисунков из двумерных сечений трехмерной фигуры, содержащих множество допустимых решений. Анализ двумерных сечений аналогичен анализу альтернатив в плоскости (см. рис. 3.3). При числе критериев более трех на оставшиеся необходимо накладывать ограничения, использовать методы свертки и сечений многомерных пространств. Так, например, при одновременной оптимизации четырех критериев получается четырехмерное пространство (пространственно-временной континуум — длина, ширина, высота и время). Оно может быть представлено в виде одномерного массива времени, элементы которого содержат трехмерное пространство на конкретный момент времени, которое, в свою очередь, сворачивается при помощи наборов двумерных сечений. Визуально это можно отобразить при помощи анимации, ви-

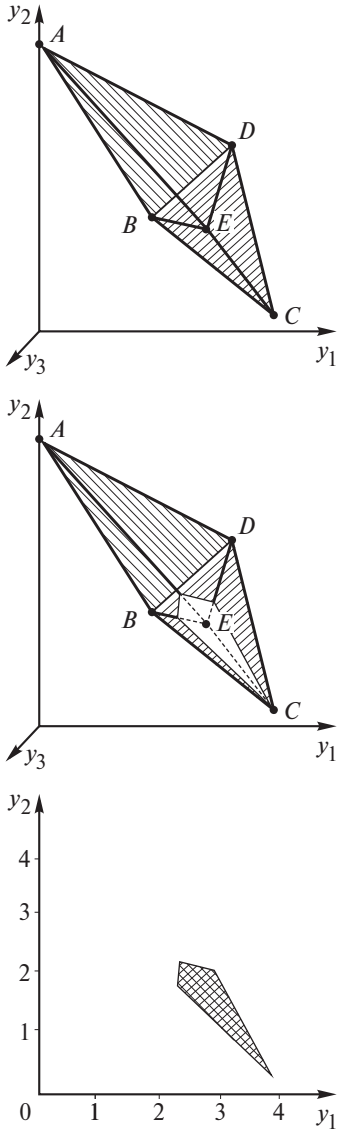


Рис. 3.4. Изображение области допустимых альтернатив для трех критериев (вверху) и двумерное сечение (внизу)

део или переключателя кадров, где каждый кадр — набор сечений в данный момент времени (под словами длина, ширина, высота, время понимаем критерии, выбранные для оптимизации); таким образом, беря значение четвертого критерия за константу, можно отобразить двумерное сечение для этой константы. В случае пяти критериев можно представить их как двумерный массив сечений, или как одномерный массив пятого критерия, элементами которого является одномерный массив четвертого критерия (время), который содержит наборы двумерных сечений (двумерное представление трехмерного объекта). В этом случае надо закреплять уже два параметра (четвертый и пятый критерии) и вычислять для этих констант двумерные сечения. Визуально их можно отобразить так: пятый критерий — ось oY, четвертый — ось oX, а точки (x, y) — двумерные сечения (вложенные графики со своими осями oX' и oY'). Дальнейшее увеличение критериев оптимизации приведет не только к проблеме визуализации, но и к проблеме нахождения оптимальной альтернативы, потому не следует выбирать более пяти критериев.

Предлагаемый метод требует компьютерной реализации в виде системы поддержки принятия решений, которая будет использовать средства визуализации и вычислительные мощности для быстрого формирования графиков, сечений, альтернатив и расчета их эффективности. Данный метод также предполагает некий подготовительный этап, в ходе которого эксперты производят поиск альтернатив, их оценку и выбор ключевых критериев для оптимизации, после чего эти сведения поступают в систему. Задача выбора альтернативных проектов построения СЗИ в пространстве описанных ранее критериев трудно формализуемая, многокритериальная и происходит в условиях частичной неопределенности (не все альтернативы и критерии заданы и описаны изначально), а значит, не поддается четкой алгоритмизации. Поэтому система поддержки принятия решений должна только делать расчеты для выбранных решений, формировать множества оптимальных решений и отображать их графически, а не принимать решение о выборе конкретной оптимальной альтернативы из построенного множества. Само принятие решения должно остаться за человеком — специалистом в области защиты информации, который, руководствуясь собственным опытом, знаниями и интуицией, сможет выбрать верное решение. Поэтому главная задача системы поддержки принятия парето-оптимальных решений в области проектирования СЗИ — помочь ЛПР принять оптимальное (компромиссное) решение в заданных условиях, причем достаточно оперативно и наглядно, а также обосновано.

Модель системы поддержки принятия парето-оптимальных решений

Для описания модели системы поддержки принятия парето-оптимальных решений будем использовать *IDEF0*-диаграмму. Контекстная диаграмма системы приведена на рис. 3.5.

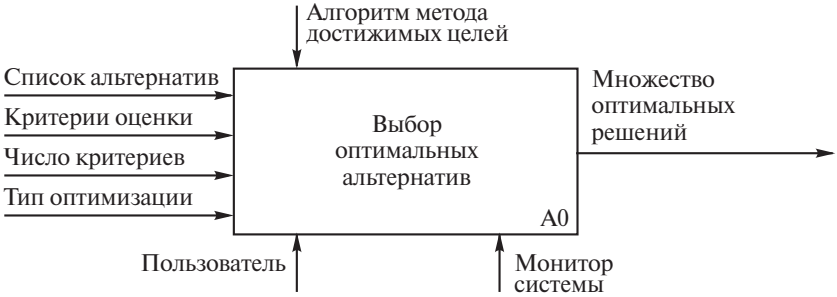


Рис. 3.5. Контекстная диаграмма системы

Проведем декомпозицию контекстной диаграммы, описав последовательность работы системы:

- выделение критериев;
- принятие решения в соответствии с правилами алгоритма МДЦ (парето-оптимизации).

Получим диаграмму, изображенную на рис. 3.6.

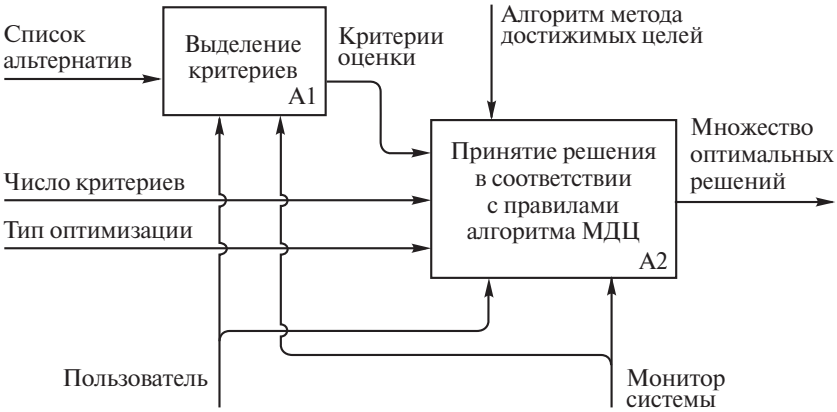


Рис. 3.6. Декомпозиция контекстной диаграммы

Из диаграмм видно, что после выбора критериев начинается процесс вычисления парето-оптимального множества и визуализации решения, по окончанию которого будет сформирован график или серия графиков, с указанием множества решений (заметим, что множество может содержать одно или более решений, но не может быть пустым). Далее пользователь может выбрать решение и получить его подробное описание, также имеется возможность поиска промежуточного решения, не указанного во входных данных, но отображаемого на графике (на линии объективного замещения).

Система поддержки принятия парето-оптимальных решений в области проектирования СЗИ решает две важные задачи: формирование множества оптимальных решений и визуальное представление этого решения. Визуализация нужна для того, чтобы стороны, участвующие в разработке СЗИ (заказчик, исполнитель и др.), могли наглядно видеть преимущества и недостатки разных проектов, вести переговоры и добиваться компромиссного решения, которое устроит всех.

Логическая модель системы поддержки парето-оптимальных решений приведена на рис. 3.7. Согласно этой модели ключевым фактором, влияющим на визуализацию решений и их поиску, является число одновременно оптимизируемых критериев. Система использует фиксированное число этих критериев: от одного до четырех включительно. Если выбран только один критерий, достаточно построить гистограмму и на значения рядов наложить кривую объективного замещения. Если выбраны два критерия, то каждый из критериев ассоциируется с осью координат, на плоскости отображаются точки-альтернативы, и по ним строится выпуклая оболочка, далее находится кривая объективного замещения.

Если выбраны три критерия, то по третьему критерию, ассоциированному с осью oZ, формируется множество двумерных сечений. Причем множество двумерных сечений строится по трем точкам, у которых третья координата (z) равна константе (для каждого сечения это разное значение). Затем производится сечение и для данного $z = \text{const}$ находятся соответствующие x и y. Число сечений ограничено снизу как число различных значений третьего критерия у всего множества альтернатив. Таким образом, можно варьировать число двумерных сечений для более детального анализа. Каждое сечение имеет свою кривую объективного замещения, которые могут совпадать. Из них формируется некая интегральная кривая с ответвлениями.

Рис. 3.7. Логическая модель системы

Точки этой кривой — оптимальные решения. Наложение двумерных сечений друг на друга с указанием значений третьего параметра на каждом сечении будем называть диалоговой картой решений.

В случае четырех критериев приходится использовать метод покадровой свертки. Четвертый критерий (его значения) будет кадром. Для каждого кадра (фиксированного значения четвертого критерия) формируется диалоговая карта решений. Для переключения между кадрами используется переключатель. Система отображает кривые объективного замещения для каждого кадра, а пользователь выбирает решение на этих кривых. Кривая может изменяться от кадра к кадру, потому надо выбрать оптимальную из всех кривую.

По выбранному решению строится отчет и выводится на экран приложения.

3.2. Порядок работы с программным инструментарием поддержки принятия парето-оптимальных решений

Описание основного рабочего окна

При запуске системы поддержки принятия парето-оптимальных решений в области проектирования СЗИ на предприятии (далее Система) появляется основное рабочее окно, содержащие две вкладки: «Список альтернатив» и «График», представленные на рис. 3.8 и 3.9 соответственно (по умолчанию открывается вкладка «Список альтернатив»).

Цифрами *1*, *2* и *3* на рис. 3.8 обозначены основные элементы управления Системой. Цифра *1* на рис. 3.8 и 3.9 отмечает область, в которой расположено основное меню Системы.

Меню содержит следующие пункты.

1. Файл:

– загрузить список альтернатив из файла;
– сохранить список альтернатив в файл;
– сохранить отчет;
– выход;

2. Справка:

– об авторе;
– о программе;
– руководство пользователя.

Цифра *2* на рис. 3.8 и 3.9 обозначает область переключателя вкладок (или страниц). Для перехода на нужную вкладку достаточно щелкнуть на ее название.

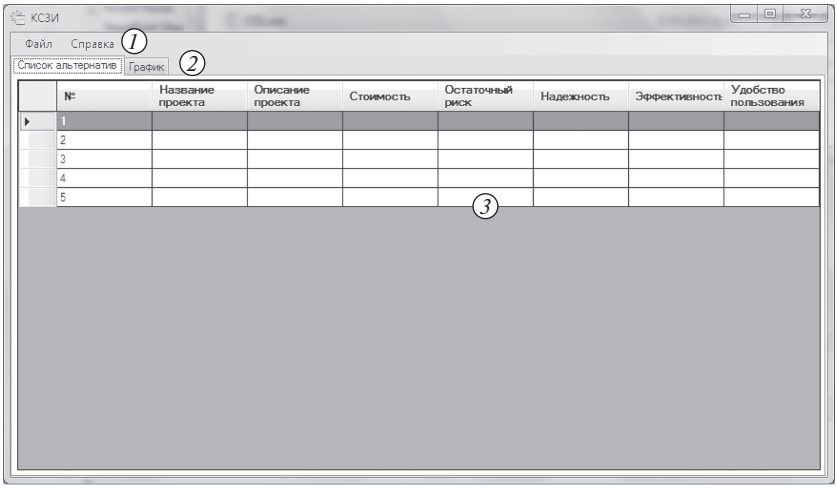


Рис. 3.8. Основное рабочее окно Система, вкладка Список альтернатив

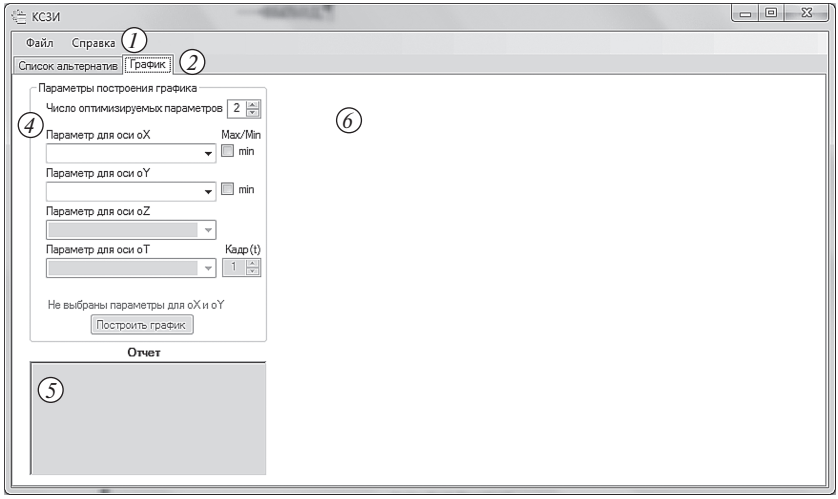


Рис. 3.9. Основное рабочее окно Системы, вкладка График

Цифра *3* на рис. 3.8 обозначает область таблицы, в которую заносятся исходные данные об альтернативных проектах СЗИ. Подробнее управление этим элемент описано в разделе Ввод исходных данных.

На рис. 3.8 изображен вид окна Системы для вкладки График.

Цифра *4* на рис. 3.9 отмечает область настройки параметров.

Цифра *5* на рис. 3.9 отмечает область вывода отчета о решении.

Цифра *6* на рис. 3.9 отмечает область построения графика (при открытии Системы область пустая). Более подробно о построении графика и настройке параметров изложено в разделе Построение графика.

Ввод исходных данных

На вкладке «Список альтернатив» основного рабочего окна Системы находится таблица для ввода данных об альтернативах (см. рис. 3.8 и 3.9). Таблица состоит из следующих столбцов:

- номер альтернативы (обозначено как №);
- название проекта;
- описание проекта;
- стоимость;
- остаточный риск;
- надежность;
- эффективность;
- удобство пользования.

Номер альтернативы заполняется программой автоматически и используется для связи описания альтернативы с ее отображением на графике. Остальные поля заполняются вручную. Все поля обязательны для заполнения, кроме поля «Описание проекта».

Название проекта должно содержать любое осмысленное и понятное пользователю название одного из нескольких альтернативных проектов. Указанное поле может содержать любые символы, общая длина его не должна превышать 255 знаков.

Описание проекта — необязательное поле, содержащее в себе описание проекта построения СЗИ, например, краткий состав его подсистем, или информацию о самом проекте (кто его разработал, когда и т.п.). Нет ограничений на длину поля.

Стоимость — поле, содержащее в себе стоимость реализации проекта в некоторой валюте (рубли, доллары, у.е.). Стоимость долж-

на быть представлена положительным числом с двумя знаками после запятой (допускается опускать знаки, если дробная часть равна нулю), сама валюта не указывается. Стоимость указывается на основании экспертной оценки как сумма стоимостей всех составных частей СЗИ с учетом текущих цен рынка, причем в стоимость входит как цена самого объекта, так и оплата дополнительных услуг по установке/монтажу и других работ, необходимых для создания функционирующей СЗИ.

Остаточный риск — поле, содержащее в себе величину риска в некоторой валюте (рубли, доллары, у.е.). Остаточный риск должен быть представлен положительным числом с двумя знаками после запятой (допускается опускать знаки, если дробная часть равна нулю), сама валюта не указывается. Остаточный риск вычисляется на основании построенной модели угроз и рисков предприятия и прогнозировании уменьшения этого риска за счет внедрения или модернизации СЗИ на основании выбранного проекта. Остаточный риск равен разности текущего уровня риска (до модернизации или создания СЗИ) и величины его уменьшения после реализации выбранного проекта. Остаточный риск характеризует риск предприятия, полученный после реализации выбранного проекта. Остаточный риск вычисляется в ходе экспертной оценке исходя из опыта и методик, выбранных экспертами.

Надежность — поле, отражающее свойство надежности СЗИ. Это комплексное свойство, включающее в себя:

- *безотказность* — свойство объекта непрерывно сохранять работоспособное состояние в течение некоторого времени или наработки;
- *ремонтопригодность* — свойство объекта, заключающееся в приспособленности к поддержанию и восстановлению работоспособного состояния путем технического обслуживания и ремонта;
- *долговечность* — свойство объекта непрерывно сохранять работоспособность от начала эксплуатации до наступления предельного состояния, т.е. такого, когда объект изымается из эксплуатации;
- *живучесть* — свойство объекта сохранять работоспособность в экстремальных ситуациях.

Надежность в таблице представляется числом от 1 до 9, где 1 означает крайне низкую надежность, 9 — очень высокую надежность,

5 — среднюю надежность, остальные числа занимают промежуточные значения. Надежность также оценивается экспертами на основании указанных ранее свойств.

Эффективность — поле, отражающее эффективность конкретного проекта СЗИ. Это степень приспособленности системы к достижению цели, являющееся комплексным свойством, включающим:

- *результативность* операций, которая обусловливается получаемым целевым эффектом, ради которого функционирует система;
- *ресурсоемкость,* характеризующаяся наличием ресурсов всех видов, используемых для получения целевого эффекта;
- *оперативность,* характеризующаяся расходом времени, потребного для достижения цели.

Эффективность в таблице представляется числом от 1 до 9, где 1 означает крайне низкую эффективность, 9 — очень высокую эффективность, 5 — среднюю эффективность, остальные числа занимают промежуточные значения. Эффективность также оценивается экспертами на основании указанных ранее свойств.

Удобство пользования — поле, показывающее, насколько данный проект СЗИ будет влиять на удобство работы с защищаемой ИС. Удобство пользования (*usability*) — это свойство системы, отражающее степень удобности использования защищенной ИС для применения пользователями при достижении определенных целей ИС. Удобство пользования в таблице представляется числом от 1 до 9, где 1 означает крайне низкую удобность пользования защищенной ИС после реализации проекта КСЗИ, 9 — очень высокую удобность пользования защищенной ИС после реализации проекта СЗИ, 5 — среднюю удобность пользования защищенной ИС после реализации проекта СЗИ, остальные числа занимают промежуточные значения. Удобство пользования защищенной ИС после реализации проекта СЗИ также оценивается экспертами, но к оценке могут привлекаться и сами пользователи.

Согласно описанным параметрам каждого альтернативного проекта, сведения вносятся в соответствующие ячейки. Один ряд таблицы полностью представляет проект СЗИ и ее основные анализируемые Системой свойства.

***Замечание 1*:** не оставляйте пустые ячейки или строки, так как в этом случае Система не сможет построить график из-за отсутствующих значений!

***Замечание 2*:** вводите в таблицу параметры стоимости, остаточного риска, надежности, эффективности и удобства пользования как число! Качественные оценки использовать нельзя! Для разделения целой и дробной частей допускается использовать в качестве разделителя точку или запятую.

Помимо описанных свойств, таблица исходных данных имеет контекстное меню, вызываемое правым щелчком мыши на таблице и содержащее следующие пункты:

– *вставить строку* (помещает новую строку под активной строкой с новым номером);
– *добавить строку в конец* (помещает пустую строку в конец таблицы с новым номером);
– *удалить строку* (удаляет выделенную строку);
– *перенумеровать строки* (нумерует все строки сверху вниз от 1 до *n*, переписывая номера).

Чтобы сделать строку активной, щелкните на ячейке этой строки или на заголовке строки справа от первой ячейки. Активные строки можно удалять и вставлять под ними новые строки при помощи команд контекстного меню.

Чтобы редактировать ячейку, дважды щелкните на ней левой клавишей мыши.

Чтобы сохранить введенный список альтернатив в файл, используйте меню Системы: нажмите Файл → Сохранить список проектов. В появившемся диалоговом окне выберите папку назначения и напишите имя файла. Файл сохраняется в текстовом формате Юникод, разделяя данные с помощью табуляции (*tab-separated text file*).

Чтобы открыть ранее сохраненный список альтернатив воспользуйтесь командой Файл → Открыть список проектов. В появившемся диалоговом окне выберите файл (*tab-separated text file*). Если выбран неверный файл, это приведет к ошибке ввода данных и может либо заполнить список пустыми строками либо вызвать исключительную ситуацию. Если выбран верный файл, то текущий список будет очищен и на его место добавлен новый список проектов, загруженный из файла.

***Внимание*!** Система анализирует лишь те проекты, которые были указаны в таблице исходных данных на вкладке «Список альтернатив» (см. рис. 3.8) на момент нажатия кнопки «Построить график» на вкладке «График» (см. рис. 3.9).

Построение графика

Для построения графика необходимо вначале заполнить таблицу исходных данных, как было описано в предыдущем разделе, а затем перейти к вкладке **График** и, выбрав параметры построения, нажать кнопку **Построить график**.

Процесс выбора параметров заключается в следующем:

- выбор уровня оптимизации (число одновременно оптимизируемых параметров — от 1 до 4);
- соотнесение параметров из выпадающих списков с осями графика;
- выбор условий минимакса (отметьте галочками те параметры, которые надо уменьшать, и уберите галочки у тех, которые надо увеличивать).

Обязательным условием во время выбора параметров является наличие связи оси графика с параметром, а также отсутствие одинаковых параметров, привязанных к разным осям. В случае допущения ошибки во время выбора будет выведено сообщение об ошибке (выделено красным) в области над кнопкой **Построить график**, а сама кнопка будет заблокирована, пока пользователь не исправит ошибку настройки параметров оптимизации.

Если все параметры выбраны верно, то кнопка «Построить график» будет разблокирована и выдано сообщение о правильном выборе параметров (выделено зеленым).

По нажатию на кнопку **Построить график** в области справа будет отображен график, а в области снизу — отчет о решении. Пример приведен на рис. 3.10.

Дополнительно при построении графика в случае уровня оптимизации, равного четырем, имеется кнопка прокрутки кадров — сечений четырехмерного пространства по значению четвертого параметра, ассоциированного с осью oT. Всего четыре кадра (от 1 до 4). Каждый кадр содержит двумерные сечения по третьему параметру (oZ), наложенные одно на другое в координатах критериев oX и oY. Подробнее о поиске оптимальных решений и их визуализации см. в разделе «Анализ графического решения».

Также у графика есть свое контекстное меню со следующими командами:

– *сглаживание*;
– *инвертировать оси*.

Сглаживание заменяет ломаные линии графика на сглаженные кривые. Инвертирование оси меняет oX и oY местами и строит график в новых координатах. Инвертирование и сглаживание недоступно для пустого графика и для уровня оптимизации равного одному. Результаты сглаживания представлены на рис. 3.11, а инвертирования осей — на рис. 3.12.

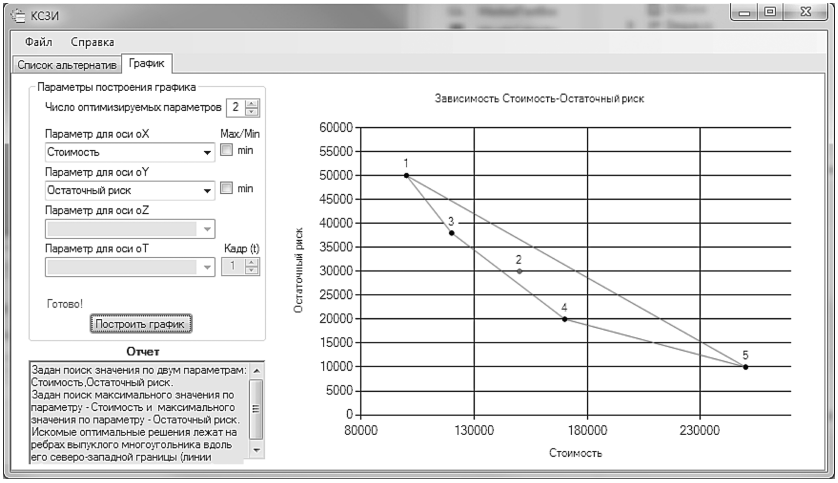


Рис. 3.10. Результаты построения графика

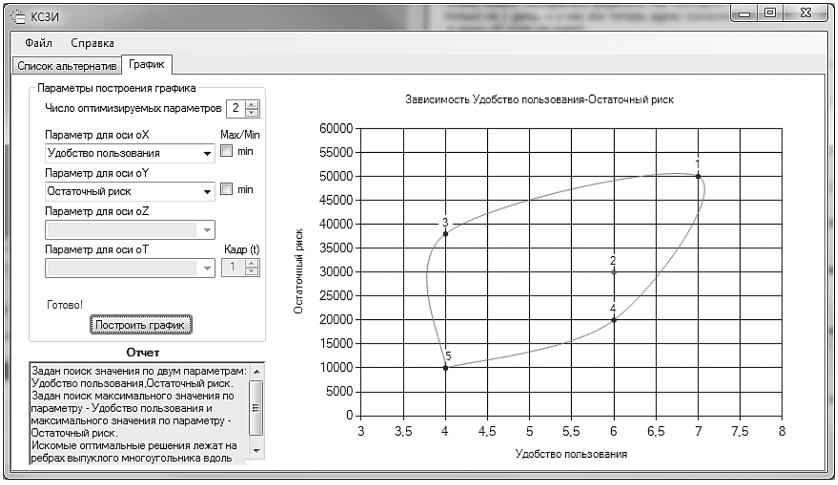


Рис. 3.11. Результат действия опции «сглаживание»контекстного меню диаграммы

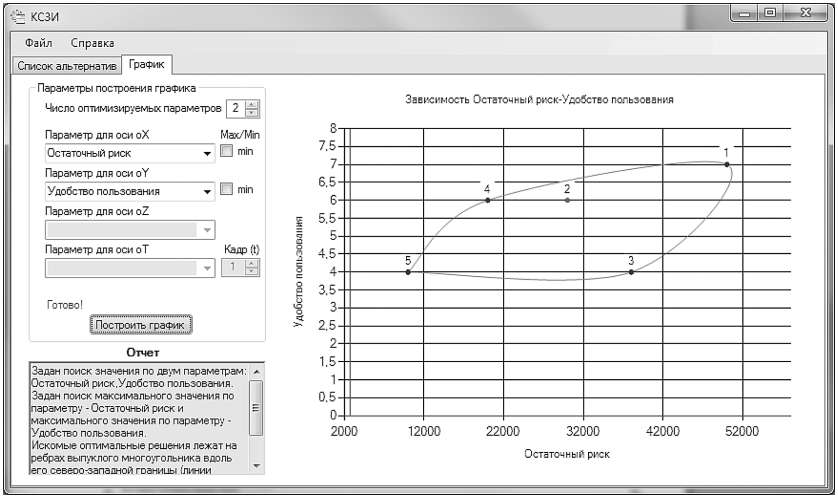


Рис. 3.12. Результат действия опции «инвертировать оси *oX* и *oY*» контекстного меню диаграммы

Анализ графического решения

После того как был построен график и сформирован отчет, пользователю необходимо выбрать из множества недоминируемых альтернатив ту, которая его больше всего устраивает.

Если оптимизация происходила по одному критерию с указанием значения поиска (минимальное или максимальное значение), то Система в отчете дает однозначный ответ, а на графике отмечает кружком правильный ответ (рис. 3.13).

Если оптимизация происходила по двум критериям, то Система строит выпуклый многоугольник в системе критериальных координат. В отчете выводится граница, вдоль которой на ребрах многоугольника находятся оптимальные решения (рис. 3.14).

Выделенными точками внутри контура отображаются неоптимальные решения (см. рис. 3.14). Точками по контуру даны оптимальные решения, парето-оптимальные решения лежат вдоль указанной границы (кривая объективного замещения). Расположение кривой зависит от того, какие параметры надо уменьшать или увеличивать и вдоль какой оси. Опишем поведение кривой для двумерной плоскости:

– *oX* и *oY* надо уменьшать, тогда кривая располагается вдоль юго-восточной границы многоугольника;

– oX и oY надо увеличивать, тогда кривая располагается вдоль северо-западной границы многоугольника;
– oX надо уменьшать, а oY — увеличивать, тогда кривая располагается вдоль северо-восточной границы многоугольника;
– oX надо увеличивать, а oY — уменьшать, тогда кривая располагается вдоль юго-западной границы многоугольника.

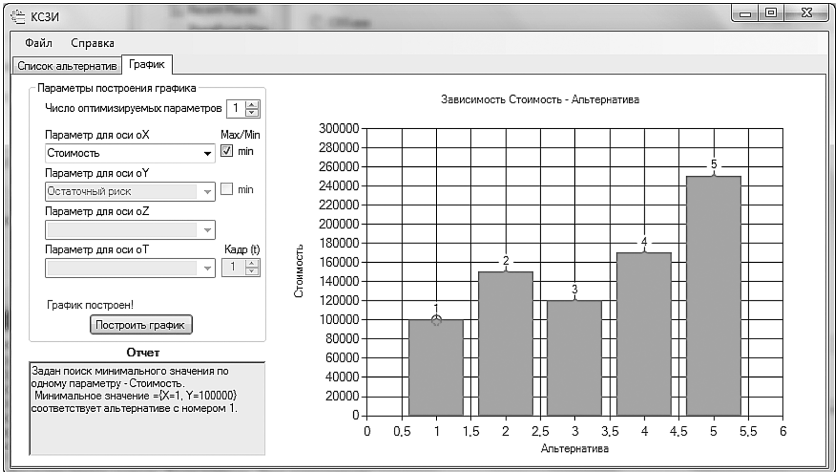


Рис. 3.13. Визуализация решения при оптимизации по одному критерию

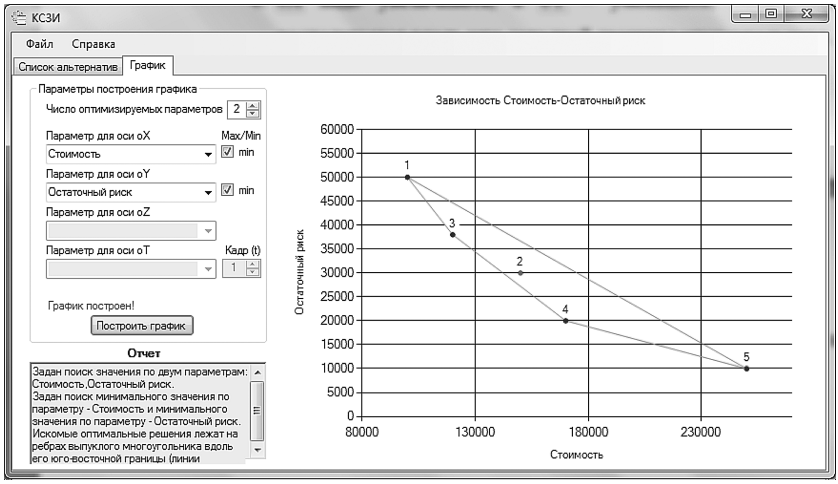


Рис. 3.14. Визуализация решения при оптимизации по двум критериям

В некоторых случаях решение будет единственным, так как указанной границе будет отчетливо принадлежать только одна точка.

В случае трех одновременно оптимизируемых параметров на графике строится наложение из двумерных сечений по третьему параметру (ось oZ). Решения ищутся так же, как и для двух критериев, с тем отличием, что в результате сечений образуются промежуточные решения, ранее не указанные в списке проектов, и указывается соответствующее им значение третьего параметра (см. рис. 3.14). Теперь нужно еще обращать внимание на значение третьего параметра и какие соответствуют ему значения параметров oX и oY.

В случае четырех одновременно оптимизируемых параметров на графике строится наложение кадров (всего четыре кадра) по четвертому параметру. Каждая отдельная точка, по сути, имеет четыре координаты, т.е. представляется в пространственно-временном континууме (рис. 3.15).

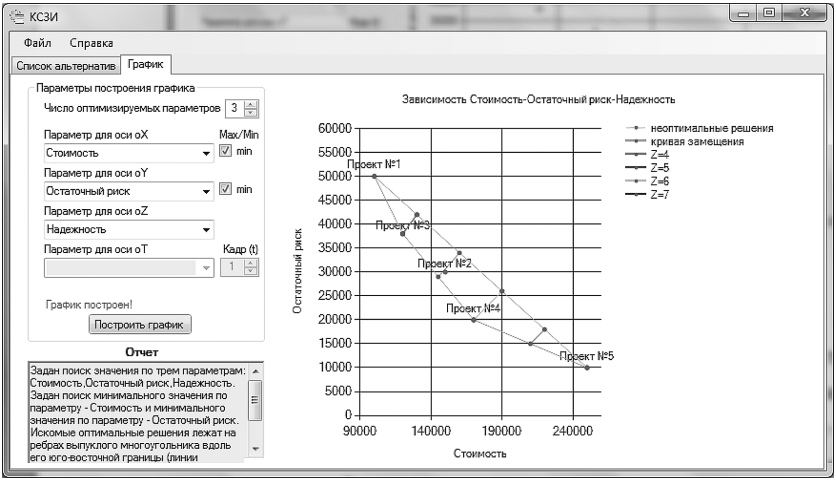


Рис. 3.15. Визуализация решения при оптимизации трех критериев

Для удобства представления все точки разделяются по кадрам, где кадр — диапазон значений четвертого критерия (диапазон указывается под параметром oT). Каждый кадр имеет в себе те решения, которые соответствуют наложенным на них ограничениям четвертого параметра (временной срез). Каждый кадр представляется как набор двумерных сечений по третьему критерию. Переключение между кадрами осуществляется специальным элементом с подписью

«Кадр (*t*)». Могут быть ситуации, когда кадр содержит ноль, одно, два или более решений (рис. 3.16).

Поиск оптимального решения похож на поиск оптимального решения для трех и двух оптимизируемых параметров с той разницей, что оптимальные решения находятся для каждого кадра, а затем выбирается лучший кадр и его лучшее решение.

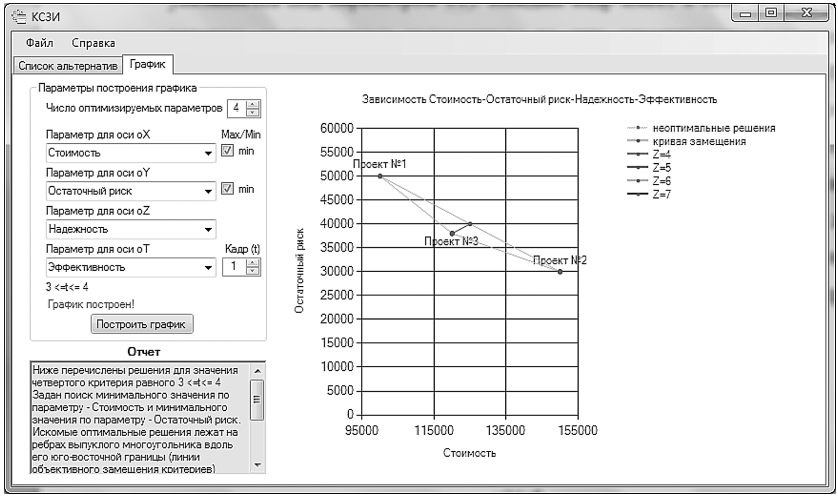


Рис. 3.16. Визуализация решения при оптимизации четырех критериев

Раздел меню Файл

Раздел меню Файл содержит команды по управлению программой, позволяющие открывать список проектов, сохранять список проектов, сохранять отчет и осуществлять выход из программы.

Функции сохранения и открытия списка проектов подробно рассмотрены в разделе **Ввод исходных данных**.

Сохранение отчета доступно по команде Файл → Сохранить отчет. При этом сохраняется весь текст отчета в файл с расширением rtf или текстовый файл по выбору пользователя. Текст файла сохраняется в формате Юникод.

Выход из программы осуществляется либо вызовом соответствующего пункта меню, либо нажатием значка «крестик» в правом верхнем углу. При выходе из программы будет запрошено подтверждение выхода (рис. 3.17).

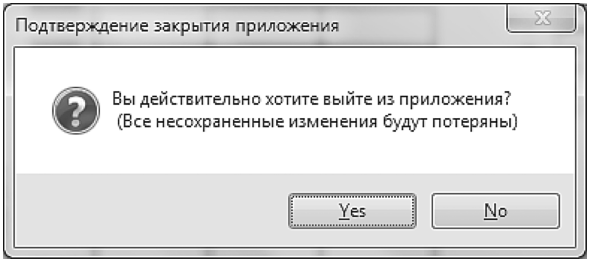


Рис. 3.17. Подтверждение выхода пользователем

Раздел меню Справка

Раздел меню Справка содержит в себе команды по вызову информации об авторе программы (рис. 3.18), о программе (рис. 3.19) и инструкции пользователя (рис. 3.20).

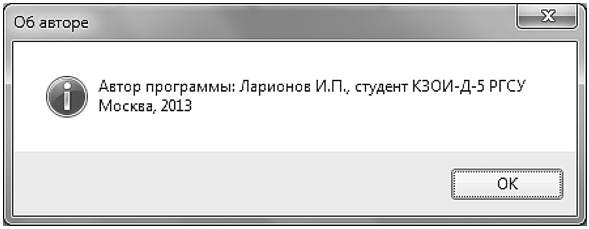


Рис. 3.18. Информация об авторе

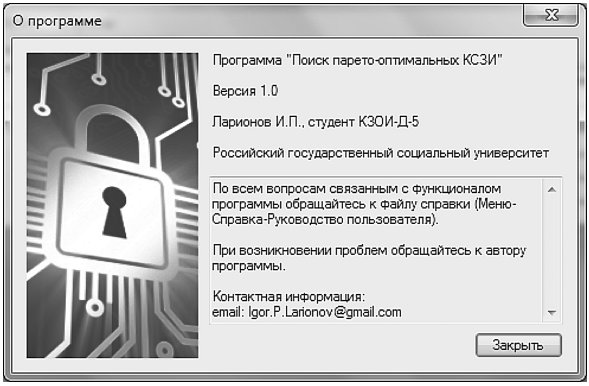


Рис. 3.19. Информация о программе

Руководство·пользователя¶

¶

по·системе·принятия·парето-оптимальных·решений·в·задачах·проектирования·комплексных·систем·защиты·информации¶¶

Рис. 3.20. Руководство пользователя

Инструкция пользователя представлена в виде *html*-файла и полностью идентична данной инструкции. Для ее прочтения требуется любой *html*-браузер. В случае если файл с инструкцией не найден, будет выдано предупреждение (рис. 3.21). В этом случае проверьте, находится ли файл справки в одном каталоге с программой.

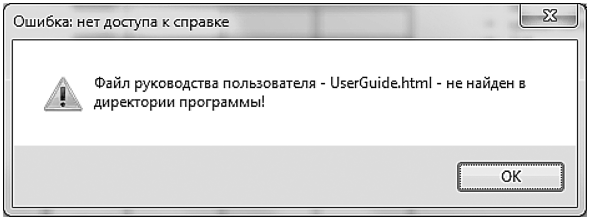


Рис. 3.21. Ошибка доступа к справке

3.3. Задания для принятия решений по оценке альтернативных проектов защиты информации на основе закона Парето и метода достижимых целей

1. Описать три альтернативных варианта СЗИ предприятия (варианты заданий см. Приложение 1). Оценки проектов занести в таблицу «Список альтернатив», руководствуясь инструкцией *Ввод исходных данных*.

2. Руководствуясь инструкцией *Построение графика*, построить графики для 2, 3 и 4 оптимизируемых параметров.

3. Руководствуясь инструкцией *Анализ графического решения*, подготовить аргументированный отчет о выборе оптимального альтернативного решения варианта СЗИ.

4. В отчете по практической работе должны быть представлены:

– схема и описание организации в соответствии в полученным вариантом;

– описание альтернативных вариантов СЗИ предприятия;
– визуализация решения при оптимизации по 2, 3 и 4 критериям;
– отчет о выборе оптимального альтернативного решения варианта СЗИ.

Контрольные вопросы и задания

1. Какие требования предъявляются к набору критериев для оценки альтернативных решений?
2. Как оценивается важность критериев?
3. Приведите классификацию задач принятия решений в области проектирования СЗИ.
4. Назовите основные этапы принятия управленческих решений в области построения защищенных систем обработки информации.
5. Приведите пример генерирования множества альтернатив с применением экспертных методов при разработке СЗИ.
6. Приведите пример использования метода строчных сумм для составления матрицы альтернативных проектов СЗИ.
7. Сформулируйте принцип Парето. В чем достоинства и недостатки его практического применения для принятия управленческих решений в области построения защищенных систем обработки информации?
8. Что понимается под парето-оптимальным множеством?
9. Какие дополнительные возможности предоставляет метод достижимых целей для принятия управленческих решений в области построения защищенных систем обработки информации?
10. Опишите последовательность шагов при использовании парето-оптимизации в выборе альтернативных проектов СЗИ.

4. АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОГО КОМПЛЕКСА ГРИФ

Цель практической работы: изучение возможностей программного комплекса ГРИФ для анализа и управления рисками ИС компаний.

Для выполнения практической работы на компьютере необходимо установить демонстрационную версию программы ГРИФ из папки *Исполняемые модули/4_ГРИФ.*

4.1. Описание программного комплекса ГРИФ для анализа и управления рисками информационных систем компаний

ГРИФ — мощный и удобный программный комплекс с интуитивно понятным интерфейсом для анализа защищенности ресурсов ИС и эффективного управления рисками. Функции программного комплекса позволяют провести анализ рисков — получить полную картину всех угроз информационной безопасности (ИБ), оценить, насколько критичны уязвимости и к каким потерям они могут привести.

Кроме анализа рисков, ГРИФ также помогает управлять ими, т.е. разрабатывать стратегию внедрения контрмер на основе анализа соотношения затраты/эффективность.

Основная задача системы ГРИФ — дать возможность самостоятельно (без привлечения сторонних экспертов) оценить уровень рисков в ИС и эффективность существующей практики обеспечения безопасности, а также предоставить возможность доказательно убедить руководство в необходимости инвестиций в сферу ИБ.

Система содержит модуль управления рисками, который позволяет проанализировать все причины того значения риска, который получается после обработки алгоритмом занесенных данных. Благодаря расчету эффективности каждой возможной контрмеры, а также определению значения остаточного риска можно выбрать оптимальные контрмеры, которые позволят снизить риск до необходимого уровня с наименьшими затратами. Работа программного комплекса состоит из пяти основных этапов.

На *первом этапе* определяют полный список информационных ресурсов, представляющих ценность для компании.

На *втором этапе* вводят в систему все виды информации, представляющей ценность для компании. Введенные группы ценной информации должны быть размещены пользователем на ранее указанных на предыдущем этапе объектах хранения информации (серверах, рабочих станциях и т.д.). Заключительная фаза — указание ущерба по каждой группе ценной информации, расположенной на соответствующих ресурсах, по всем видам угроз.

На *третьем этапе* вначале определяют все виды пользовательских групп. Затем выясняют, к каким группам информации на ресурсах имеет доступ каждая из групп пользователей. В заключение определяют виды (локальный и/или удаленный) и права (чтение, запись, удаление) доступа пользователей ко всем ресурсам, содержащим ценную информацию.

На *четвертом этапе* требуется указать, какими средствами защищена ценная информация на ресурсах и рабочих местах групп пользователей. Также вводится информация о разовых затраты на приобретение всех применяющихся средств защиты информации и о ежегодных затратах на их техническую поддержку, а также — о ежегодных затратах на сопровождение системы информационной безопасности компании, куда включаются затраты на годовую зарплату персонала, занимающегося вопросами обеспечения ИБ; обучение персонала по ИБ; услуги в области ИБ сторонних компаний; сертификация в области ИБ, и т.д.

Пример создания проекта в системе ГРИФ представлен на рис. 4.1.

На *завершающем этапе* пользователь должен ответить на ряд вопросов по политике безопасности, реализованной в системе, что позволяет оценить реальный уровень защищенности системы и детализировать оценки рисков. Этот этап необходим для получения достоверных оценок существующих в системе рисков. Применение средств информационной защиты не делает систему защищенной в случае их неадекватного использования и отсутствия комплексной политики безопасности, учитывающей все аспекты защиты информации, включая вопросы организации защиты, физической безопасности, безопасности персонала, непрерывности ведения бизнеса и т.д.

Пример формирования раздела «*Управление рисками*» приведен на рис. 4.2.

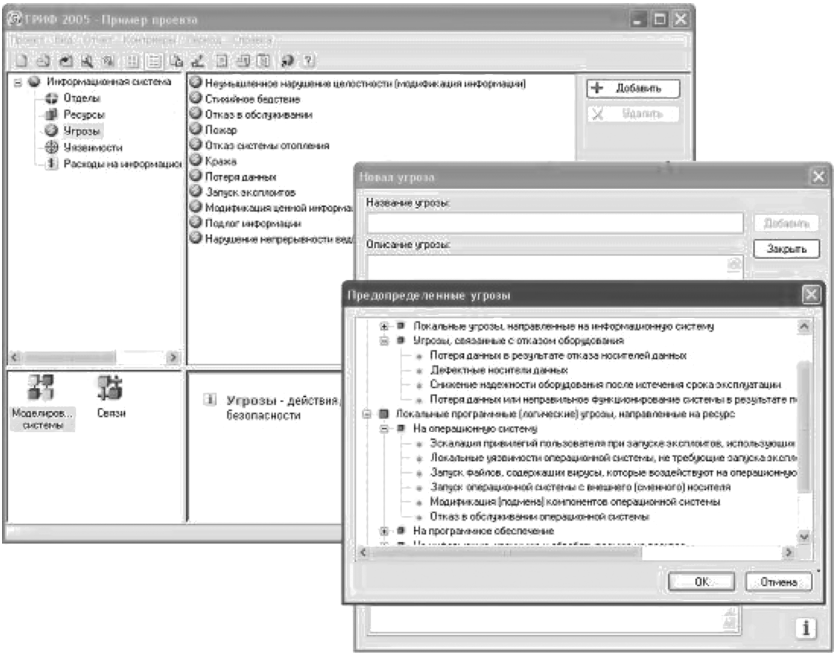


Рис. 4.1. Пример создания проекта в системе ГРИФ

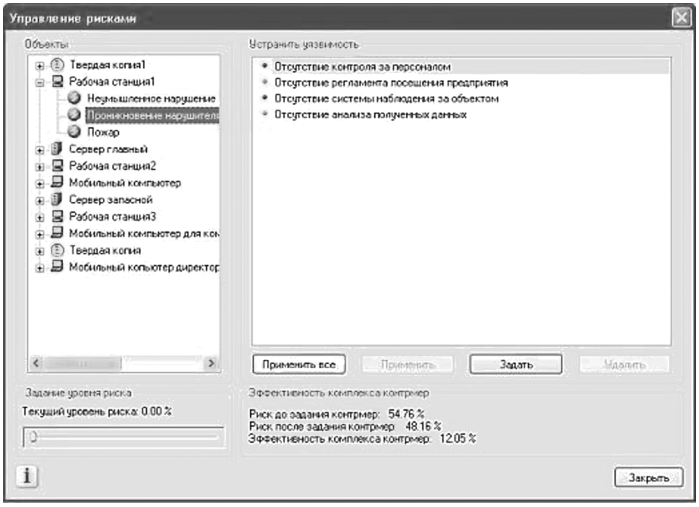


Рис. 4.2. Пример формирования раздела «*Управление рисками*»

После ввода ответов на вопросы раздела «*Политика безопасности*» будет сформирована полная модель ИС с позиции ИБ с учетом реального выполнения требований комплексной политики безопасности.

Отчет, получаемый на выходе, состоит из трех частей.

Первая часть отчета — «*Информационные риски ресурсов*».

- Информационные риски ресурсов по информации и классу угроз.
- Информационные риски ресурсов по классу угроз.
- Информационные риски ресурсов, суммарные риски по ресурсам.
- Информационные риски системы по классу угроз.

Вторая часть отчета — «*Соотношение ущерба и риска*».

- Ущерб по ресурсам по информации и по классу угроз.
- Ущерб по ресурсам, суммарный ущерб по ресурсам.
- Ущерб и риск системы по классу угроз.
- Ущерб и риск системы.
- Риск системы и затраты на обеспечение ИБ системы.

Третья часть отчета — «*Общий вывод о существующих рисках информационной системы*»:

- Максимальные значения риска и ущерба.
- Недостатки существующей политики безопасности.

4.2. Пример анализа рисков информационной безопасности в системе дистанционного банковского обслуживания «Банк-Клиент» с использованием комплекса ГРИФ

Анализ угроз и уязвимостей

Анализ угроз и уязвимостей проводим по методике, реализованной в программной системе *Digital Security Office* ГРИФ 2006 по алгоритму «*Анализ модели угроз и уязвимостей*».

Для построения модели угроз и уязвимостей в программу заносят данные об исследуемой системе дистанционного банковского обслуживания (ДБО) Банк-Клиент:

- ресурсы, используемые для хранения и обработки защищаемой информации;
- угрозы, действующие на ресурсы системы;
- уязвимости, присутствующие в системе.

Экспертные оценки уровней (конфиденциальности, целостности, доступности) получены в результате опроса в подразделениях сопровождения системы ДБО Банк-Клиент и ИБ банка.

Результат анализа угроз и уязвимостей системы ДБО Банк-Клиент можно рассмотреть с помощью таблиц по объектам хранения и обработки защищаемой информации:

– для серверов СУБД, АБС, приложений;
– для Web-сервера;
– для рабочих мест сотрудников банка;
– для рабочих мест сотрудников клиентов (в офисе, дома, мобильных, гостевых);
– для носителей ключевой информации клиентов.

Рассмотрим угрозы и уязвимости банковской части системы ДБО Банк-Клиент (табл. 4.1–4.3).

Таблица 4.1

Серверы СУБД, АБС, приложений

Угроза	*Уязвимость*	*Конфиденциальность, уровень*	*Целостность, уровень*	*Доступность, уровень*
Ошибки, не регламентированные действия, НСД	Недостаточная информированность и/или квалификация	1	1	1
	Неадекватное разделение прав доступа	1	1	1
Нестабильное функционирование серверов	Неправильная конфигурация, несвоевременная установка обновлений	1	1	1
	Отсутствие дублирования аппаратного обеспечения, ИБП	1	1	1
	Отсутствие возможности оперативного восстановления ПО и данных	1	1	1

Таблица 4.2

Web-сервер системы ДБО Банк-Клиент

Угроза	*Уязвимость*	*Конфиденциальность, уровень*	*Целостность, уровень*	*Доступность, уровень*
Ошибки, нерегламентированные действия, НСД	Недостаточная информированность и/или квалификация	1	1	1
	Неадекватное разделение прав доступа	1	1	1
Нестабильное функционирование серверов	Неправильная конфигурация, несвоевременная установка обновлений	1	1	1
	Отсутствие дублирования аппаратного обеспечения, ИБП	1	1	1
	Отсутствие возможности оперативного восстановления программного обеспечения (ПО) и данных	1	1	1
Преднамеренные действия и НСД мошенника	Применение стандартного ПО системы ДБО Банк-Клиент	1	1	1

Таблица 4.3

Рабочие места сотрудников банка

Угроза	*Уязвимость*	*Конфиденциальность, уровень*	*Целостность, уровень*	*Доступность, уровень*
Ошибки, нерегламентированные действия, НСД	Недостаточная информированность и/или квалификация	2	1	1
	Неадекватное разделение прав доступа	2	1	1

Рассмотрим угрозы и уязвимости клиентской части системы ДБО Банк-Клиент (табл. 4.4–4.7).

Таблица 4.4

Рабочие места сотрудников клиентов в офисе

Угроза	*Уязвимость*	*Конфиденциальность, уровень*	*Целостность, уровень*	*Доступность, уровень*
Выманивание ключей ЭП и паролей, подмена ссылки на сайт ДБО Банк-Клиент	Недостаточная информированность и/или квалификация	1	1	1
Внедрение вирусов, программ-шпионов, удаленное управление	Несвоевременная установка критичных обновлений	1	1	1
	Отсутствие лицензионного антивируса	1	1	1
	Неадекватное разделение прав доступа	1	1	1

Таблица 4.5

Мобильные рабочие места сотрудников клиентов

Угроза	*Уязвимость*	*Конфиденциальность, уровень*	*Целостность, уровень*	*Доступность, уровень*
Выманивание ключей ЭП и паролей, подмена ссылки на сайт ДБО Банк-Клиент	Недостаточная информированность и/или квалификация	1	1	1
Внедрение вирусов, программ-шпионов, удаленное управление	Несвоевременная установка критичных обновлений	1	1	1
	Отсутствие лицензионного антивируса	1	1	1
	Неадекватное разделение прав доступа	1	1	1

Таблица 4.6

Домашние и гостевые рабочие места сотрудников клиентов

Угроза	*Уязвимость*	*Конфиденциальность, уровень*	*Целостность, уровень*	*Доступность, уровень*
Выманивание ключей ЭП и паролей, подмена ссылки на сайт ДБО Банк-Клиент	Недостаточная информированность и/или квалификация	1	1	1
Внедрение вирусов, программ-шпионов, удаленное управление	Несвоевременная установка критичных обновлений	2	2	1
	Отсутствие лицензионного антивируса	2	2	1
	Неадекватное разделение прав доступа	2	2	1

Таблица 4.7

Носитель ключевой информации клиентов

Угроза	*Уязвимость*	*Конфиденциальность, уровень*	*Целостность, уровень*	*Доступность, уровень*
Ошибки, нерегламентированные действия, НСД	Недостаточная информированность и/или квалификация	2	2	2
Компрометация ключей ЭП (копирование, потеря, удаленный перехват)	Применение незащищенного носителя ключевой информации	2	2	2
	Отсутствие личной ответственности и разграничения доступа	1	1	1

Рассмотрим суммарные уровни угроз для банковской и клиентской частей системы ДБО Банк-Клиент (табл. 4.8).

Таблица 4.8

Суммарные уровни угроз по ресурсам

Ресурс	*Конфиденциальность, уровень*	*Целостность, уровень*	*Доступность, уровень*	*Итого, уровень*
Серверы СУБД, АБС, приложений	3	3	3	5
Web-сервер системы ДБО Банк-Клиент	3	3	3	5
Рабочие места сотрудников банка	2	2	2	4
Рабочие места сотрудников клиентов в офисе	3	3	2	4
Мобильные рабочие места сотрудников клиентов	3	2	2	4
Домашние и гостевые рабочие места сотрудников клиентов	4	4	2	5
Носитель ключевой информации клиентов	3	3	3	5

На основании табл. 4.8 можно сделать вывод о практически одинаково высоком итоговом уровне угроз для всех ресурсов системы ДБО Банк-Клиент.

Анализ рисков

Условные обозначения и номера ресурсов системы ДБО Банк-Клиент, применяемые в сформированных графиках:

1 — серверы СУБД, АБС, приложений;
2 — Web-сервер системы ДБО Банк-Клиент;
3 — рабочие места сотрудников банка;
4 — рабочие места сотрудников клиентов в офисе;
5 — мобильные рабочие места сотрудников клиентов;
6 — домашние и гостевые рабочие места сотрудников клиентов;
7 — носитель ключевой информации клиентов;
К — конфиденциальность;
Ц — целостность;
Д — доступность;
И — итого.

Рассмотрим показатели риска в банковской части системы ДБО Банк-Клиент (табл. 4.9, рис. 4.3).

Таблица 4.9

Суммарные риски по ресурсам в банке

Ресурс	*Значение риска*, %
Серверы СУБД, АБС, приложений	88,71
Web-сервер системы ДБО Банк-Клиент	89,50
Рабочие места сотрудников банка	70,98

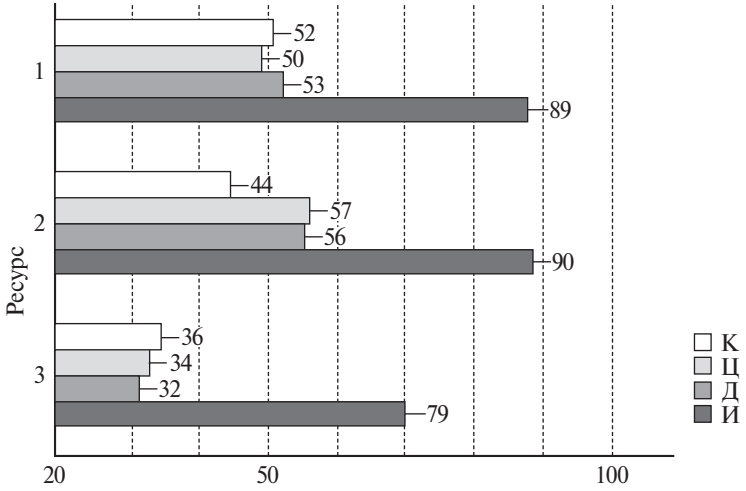


Рис. 4.3. Анализ риска в банковской части системы ДБО Банк-Клиент

Рассмотрим показатели риска в клиентской части системы ДБО Банк-Клиент (табл. 4.10, рис. 4.4).

Таблица 4.10

Суммарные риски по ресурсам у клиентов

Ресурс	*Значение риска*, %
Рабочие места сотрудников клиентов в офисе	77,85
Мобильные рабочие места сотрудников клиентов	76,04
Домашние и гостевые рабочие места сотрудников клиентов	91,27
Носитель ключевой информации клиентов	90,89

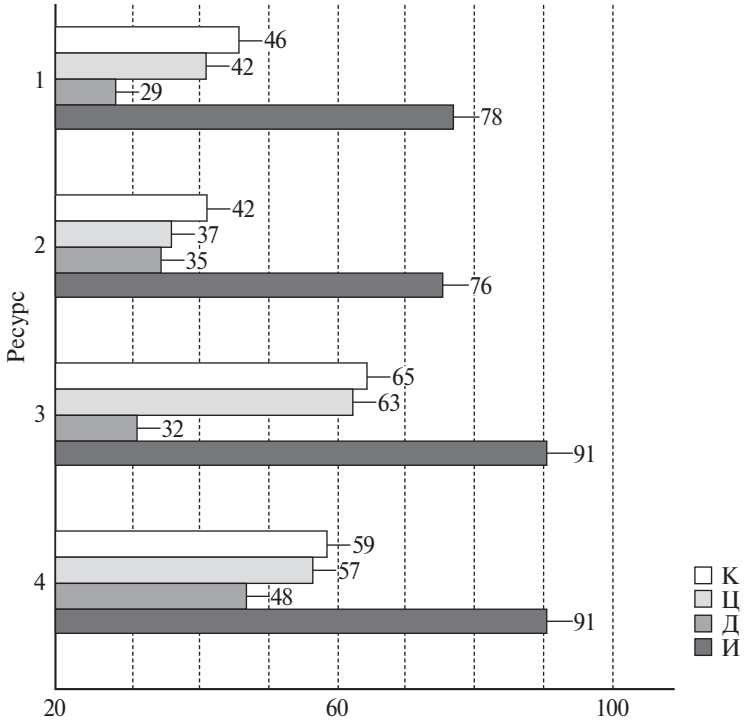


Рис. 4.4. Анализ риска в клиентской части системы ДБО Банк-Клиент

На основе суммарных значений рисков по ресурсам системы ДБО Банк-Клиент можно сделать выводы о необходимости дополнительной защиты информации, хранимой и обрабатываемой на серверах в банке, и носителей ключевой информации клиентов.

4.3. Задания для анализа и управления рисками компании с использованием комплекса ГРИФ

1. Установить на своем компьютере демонстрационную программу ГРИФ 2006 (файл *dsoffice2006_pe_demo.msi*). Запустить программу, для чего необходимо авторизоваться в начальном окне запуска.

2. Для рассматриваемого в описании предприятия (Приложение 3) получить отчет в программе ГРИФ с использованием алго-

ритма «*Анализ модели информационных потоков*». Исходными материалами для отчета являются данные о всех ресурсах ИС предприятия, группах пользователей, правах и видах доступа к информационным ресурсам.

3. Для рассматриваемого в описании предприятия (Приложение 3) получить отчет в программе ГРИФ с использованием алгоритма «*Анализ модели угроз и уязвимостей*». Оценить риски каждого ресурса ИС рассматриваемого предприятия. Исходными материалами для получения отчета являются перечни угроз и уязвимостей для каждого ресурса ИС (с возможностью выбора из типовых вариантов).

4. Предоставить отчеты по п. 2 и п. 3.

Контрольные вопросы и задания

1. Какие возможности предоставляет программный комплекс ГРИФ для анализа и управления рисками ИС компаний?
2. Какие программные инструментарии можно рекомендовать для анализа и управления рисками ИБ для крупных государственных компаний?
3. Какие программные инструментарии можно рекомендовать для анализа и управления рисками ИБ для мелких коммерческих компаний с ограниченными финансовыми возможностями?
4. Для каких целей при управлении рисками ИБ может использоваться алгоритм «*Анализ модели информационных потоков*» программного комплекса ГРИФ?
5. Для каких целей при управлении рисками ИБ может использоваться алгоритм «*Анализ модели угроз и уязвимостей*» программного комплекса ГРИФ?
6. Какими достоинствами и недостатками обладает программный комплекс ГРИФ?
7. Назовите основные этапы анализа рисков ИБ, используемые в программном комплексе ГРИФ.
8. Какие выводы можно сделать на основе анализа суммарных значений рисков по ресурсам ИС?
9. Какое влияние на формирование выходного отчета в программе ГРИФ оказывает полнота и адекватность исходных данных?
10. Оцените возможности визуализации результатов в выходном отчете программного комплекса ГРИФ.

5. РАЗРАБОТКА СЦЕНАРИЕВ ДЕЙСТВИЙ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ СЕТИ ПЕТРИ

Цель практической работы: изучение возможностей моделирования на основе сетей Петри для построения сценариев действий нарушителя на объекте информатизации.

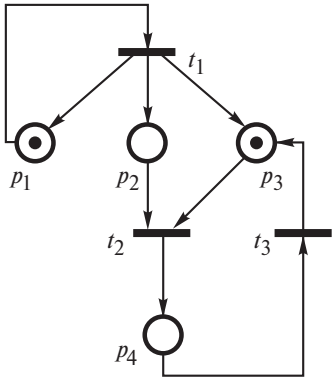
Для выполнения практической работы на компьютере необходимо запустить программу *VisualPetri* из папки: *Исполняемые модули/5_Сети Петри*.

5.1. Особенности моделирования на основе сети Петри

Сети Петри — это ориентированные графы с выделенными вершинами двух типов:

- условия-позиции;
- события-переходы.

В качестве графического средства сети Петри могут использоваться для наглядного представления моделируемой системы подобно блок-схемам, структурным схемам и сетевым графикам. Вводимое в этих сетях понятие фишек позволяет моделировать динамику функционирования систем и параллельные процессы. В качестве математического средства аналитическое представление сети Петри позволяет составлять уравнения состояния, алгебраические уравнения и другие математические соотношения, описывающие динамику систем. Моделирование в сетях Петри осуществляется на событийном уровне. Определяется, какие действия происходят в системе, какие состояния предшествовали этим действиям и какие состояния примет система после выполнения действия. Выполнения событийной модели в сетях Петри описывает поведение системы. Анализ результатов выполнения может дать представление о том, в каких состояниях пребывала или не пребывала система, какие состояния в принципе недостижимы. Однако такой анализ не дает числовых характеристик, определяющих состояние системы.



$C = (1\ 0\ 1\ 0)$

Рис. 5.1. Вектор текущего состояния сети Петри

Сети Петри имеют удобную графическую форму представления в виде графа, в котором позиции изображаются кружками, а переходы — прямоугольниками. Позиции и переходы соединяются направленными дугами (рис. 5.1).

Сеть Петри позволяет моделировать динамические и дискретные процессы. Моделирование динамического хода системы осуществляется с помощью фишек или маркеров, которые представляются в позиции в виде точек. Размещение фишек в позиции называется маркировкой. Отсутствие меток в некоторой позиции свидетельствует о нулевой маркировке этой позиции. Изменение маркировки описывается с помощью запуска с заданным правилом запуска.

Правило запуска

Если переход разрешен, т.е. все входные позиции этого перехода маркированы, по крайней мере, одной фишкой, то переход можно запускать. Запуск удаляет из каждой входной позиции одну фишку и добавляет одну фишку в каждую выходную позицию.

Пусть C — сеть Петри;
P — множество позиций в C;
T — множество переходов в C;
$n(P)$ — число позиций в P.

Каждая позиция в C однозначно связана с номером из набора номеров 1, 2, ..., $n(P)$. Тогда разметку сети можно представить как вектор, состоящий из $n(P)$ элементов, в котором i-й элемент означает число пометок в i-й позиции.

Сети Петри могут применяться в самых разнообразных областях:

- *для моделирования бизнес-процессов*. Функциональные диаграммы в нотации *IDEF3* могут быть преобразованы в сеть Петри. Каждой работе на диаграмме соответствует переход сети Петри. Позиции соответствуют стрелкам, соединяющим

работы напрямую, и перекресткам. Метки соответствуют продукции, документам и т.д., причем в зависимости от перехода интерпретация метки может отличаться;

- *для моделирования параллельных вычислений и устройств*. Если представить себе переход как процедуру, то она корректно выполняется при наличии значений всех своих аргументов и вырабатывает значения всех выходных переменных. В таком случае входные позиции перехода соответствуют аргументам, выходные — возвращаемым значениям. В другой интерпретации переход может представлять некоторое устройство, которое может (но не должно) сработать, если выполнились все входные условия;
- *для создания динамических сценариев*. Тогда позиция соответствует некоторому состоянию объекта, метка сопоставляется ресурсу, а переход ассоциируется с процессом преодоления препятствия.

5.2. Порядок работы с программным модулем *VisualPetri*

Модуль *VisualPetri* может использоваться для моделирования процессов в системе защиты информации с использованием сетей Петри и, в частности, для построения сценария действий нарушителя.

В состав комплекса программ входят следующие файлы и папки, краткое описание которых можно найти в табл. 5.1.

Таблица 5.1

Файлы и папки комплекса программ

Тип	*Имя*	*Краткое описание*
Папка	*Data*	Общие данные, в основном графические файлы
Папка	*Local*	Локальные настройки пользователя
Папка	*Samples*	Примеры
Файл	*BCGCB.dll*	Компонент *BCGControlBar*
Файл	*Config.ini*	Внутренние настройки программы *VisualPetri*
Файл	*VisualPetri.exe*	Программа *VisualPetri*

Однако для корректной работы комплекса программ необходимо наличие еще двух файлов (табл. 5.2), которые должны находиться либо в папке комплекса программ, либо в папке *C:\Windows\System*.

Таблица 5.2

Дополнительные файлы

Тип	*Имя*	*Краткое описание*
Файл	*GDIPlus.dll*	*Microsoft Graphical Device Interface*
Файл	*MFC42.dll*	*Microsoft Foundation Classes*

При запуске из каталога комплекса программ файла *VisualPetri.exe* появляется основное окно программы, вид которого приведен на рис. 5.2.

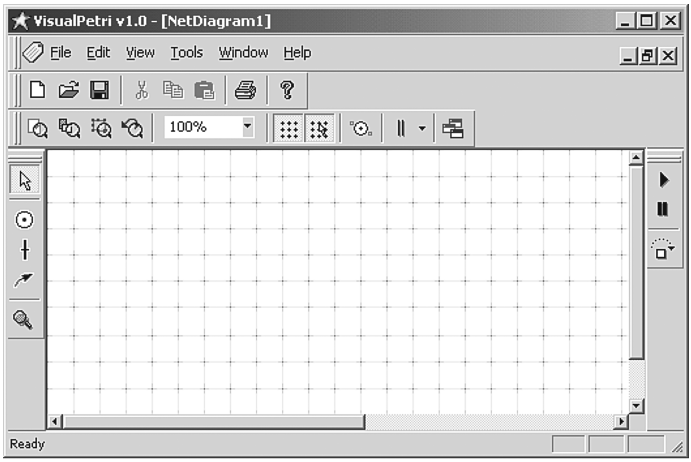


Рис. 5.2. Основное окно программы *VisualPetri*

Рассмотрим элементы основного окна: меню и панели инструментов.

В меню программы (рис. 5.3) входят следующие команды:

File — операции загрузки, сохранения диаграмм, распечатки на принтере, выхода из программы;

Edit — операции с содержимым диаграммы;

View — перерисовка содержимого диаграммы, отображение логической сетки, панелей инструментов, настройка их и меню;

Tools — вызов окна опций программы;

Window — управление открытыми окнами;

Help — справка о разработчике.

Рис. 5.3. Меню программы *VisualPetri*

На рис. 5.4 изображена панель инструментов *Standard*. В состав этой панели входят команды:

1 — открыть диаграмму;
2 — открыть папку;
3 — сохранить текущую диаграмму;
4 — нефункциональные элементы;
5 — печать активной диаграммы;
6 — вызов диалогового окна «О программе».

Рис. 5.4. Панель инструментов *Standard*

На рис. 5.5 представлена панель инструментов *Diagram*. Эта панель состоит из следующих команд:

1 — показать всю диаграмму (масштабировать в окне);
2 — показать содержимое диаграммы (масштабировать в окне);
3 — показать выделение (масштабировать в окне);
4 — вернуться к предыдущему масштабу;
5 — масштаб в процентах;
6 — отображать/прятать сетку;
7 — привязываться или нет к логической сетке;
8 — показывать или нет соединительные маркеры у всех элементов;
9 — направление создания сети (при добавлении новых элементов): вертикальное (соединительные маркеры выстраиваются вертикально) или горизонтальное (соединительные маркеры выстраиваются горизонтально);
10 — открыть новое окно просмотра текущей диаграммы.

Рис. 5.5. Панель инструментов *Diagram*

На рис. 5.6 изображена панель инструментов *Elements*. Она состоит из команд:

1 — вкл./выкл. режима выбора элементов диаграммы;
2 — вкл./выкл. режима добавления в сеть позиций;
3 — вкл./выкл. режима добавления в сеть переходов;
4 — вкл./выкл. режима соединения элементов сети Петри дугами;
5 — вкл./выкл. режима масштабирования отдельных областей мышью.

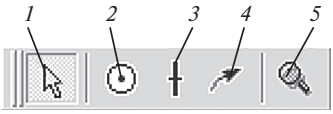


Рис. 5.6. Панель инструментов *Elements*

И наконец, последняя панель инструментов, показанная на рис. 5.7, называется *Run*. Входящие в нее команды:

1 — запустить на выполнение активную сеть Петри;
2 — приостановить выполнение;
3 — трассировка (пошаговое выполнение).

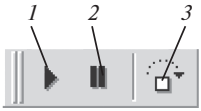


Рис. 5.7. Панель инструментов *Run*

Процесс создания сети начинается с добавления функциональных элементов сети Петри на диаграмму. Рекомендуется сначала расположить позиции (если вы хорошо представляете, как будет выглядеть сеть), затем — переходы и уже потом приступить к их соединению дугами.

Нажав соответствующую элементу кнопку на панели инструментов *Elements,* поместите курсор мыши в ту точку области редактирования, куда необходимо добавить элемент, затем нажмите левую кнопку мыши. Следите за правильностью создаваемой сети, чтобы впоследствии она без проблем выполнялась.

Чтобы добавить фишки в построенную сеть, необходимо нажать кнопку вкл./выкл. добавления в сеть позиции на панели *Elements* (см. рис. 5.6), навести курсор мыши на ту позицию, куда требуется добавить фишку, и нажать левую кнопку мыши.

Для удобства редактирования используйте масштабирование, задавайте направление создания сети, чтобы в будущем не поворачивать соединительные маркеры в противоположную сторону.

В процессе редактирования не забывайте сохранять файл. Удобнее всего это делать клавиатурным сокращением **Ctrl + S** или командами **Save** и **Save As**, входящими в пункт меню **File.**

5.3. Задания для построения сценария действий нарушителя на объекте информатизации с использованием сети Петри

1. Описать структуру малого предприятия с указанием перечня помещений и оборудования, используемого для обработки защищаемой информации (варианты предлагаются преподавателем), см. Приложение 1.

2. Провести анализ угроз. При анализе ИБ обязательным условием является построение полного множества угроз. Каждая конкретная угроза должна рассматриваться в следующем порядке: чему она угрожает, как обнаруживается, частота ее проявления, последствия, как предотвращается. Составить полную матрицу угроз.

3. Разработать сценарий действий потенциального нарушителя на объекте информатизации. Для наглядного представления действий нарушителя при достижении наиболее критичных информационных ресурсов использовать сеть Петри, для чего запустить программу *VisualPetri*. Руководствуясь описанием малого предприятия (Приложение 1), построить сеть Петри, соответствующую процессу развития атаки. Маркировать полученную сеть и серией последовательных запусков определить достижимость конечных целей.

4. Привести в отчете структуру разработанной сети Петри и подробное описание позиций и переходов в разработанном сценарии. Проанализировав работу сети, сделать выводы о достижимости конечных целей атак.

Контрольные вопросы и задания

1. В чем отличие сетей Петри от других способов моделирования в системах защиты информации?
2. Каким образом можно интерпретировать позиции и переходы при разработке сценариев действия нарушителя на объекте информатиз ации с использованием сети Петри? Приведите конкретные примеры.
3. В чем заключается ограниченность использования сетей Петри для моделирования процессов, происходящих в ИС?
4. Каким образом можно интерпретировать использование маркеров в сети Петри при моделировании действий нарушителя? Приведите конкретные примеры.
5. Какие выводы можно сделать о достижимости конечной цели атак при запуске разработанной сети Петри?

6. ОПРЕДЕЛЕНИЕ ПОКАЗАТЕЛЕЙ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ПРИ НЕСАНКЦИОНИРОВАННОМ ДОСТУПЕ

Цель практической работы: Определить показатели защищенности информации при несанкционированном доступе к информационной системе с несколькими оболочками защиты. Провести анализ зависимости показателя уязвимости информации от параметров системы защиты.

6.1. Методы расчета прочности оболочки защиты

Основная сложность функционального построения системы защиты информации — доля нечетко определенных исходных данных; большое число механизмов защиты; сложность их взаимных связей и многие другие факторы, что делает чрезвычайно затруднительной проблему оценки эффективности системы защиты в целом с помощью одного какого-либо метода моделирования.

Для решения этой проблемы применяется способ декомпозиции задачи оценки эффективности защищенности системы на ряд частных подзадач, например:

- оценка эффективности защиты от сбоев и отказов аппаратных и программных средств;
- оценка эффективности защиты от несанкционированного доступа;
- оценка эффективности защиты от побочных электромагнитных излучений и наводок (ПЭМИН) и т.д.

При оценке эффективности защиты от отказов, приводящих к уничтожению информации, используется, например, такая величина как вероятность безотказной работы $P(t)$ системы за время t. Этот показатель вычисляется по формуле

$$P(t) = 1 - P_{\text{отк}}(t),$$

где $P_{\text{отк}}(t)$ — вероятность отказа системы за время t.

В свою очередь, величина $P_{\text{отк}}(t)$ вычисляется по известному выражению

$$P_{\text{отк}}(t) = \mathrm{e}^{-\lambda t},$$

где λ — интенсивность отказов системы.

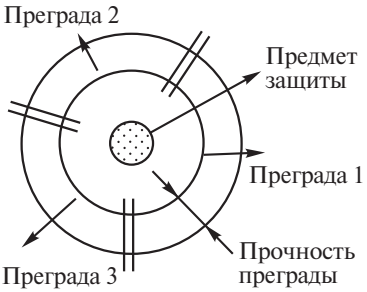


Рис. 6.1. Схема многозвенной защиты объекта информатизации

В связи с построением современных систем защиты информации характерно использование вариантов многозвенной защиты (рис. 6.1).

Считается, что прочность преграды достаточна, если стоимость ожидаемых затрат на ее преодоление потенциальным нарушителем превышает стоимость защищаемой информации. Однако на практике используется другой подход к оценке прочности преграды. Прочность преграды оценивается вероятностью ее преодоления или обхода потенциальным нарушителем по пути с наибольшим значением этой вероятности. Другими словами, прочность защиты $P_{\text{СЗИ}}$ определяется ее слабейшим звеном:

$$P_{\text{СЗИ}} = 1 - P_{\text{НР}},$$

где $P_{\text{НР}}$ — вероятность преодоления преграды нарушителем.

На практике необходимо учитывать вероятность обхода преграды $P_{\text{обх}}$. При рассмотрении одиночного нарушителя, очевидно, выбирается один из путей: преодоление преграды или ее обход. Тогда, учитывая несовместимость событий, формальное выражение для прочности преграды можно представить в виде:

$$P_{\text{СЗИ}} = \min\{(1 - P_{\text{НР}}), (1 - P_{\text{обх}})\}.$$

У преграды может быть несколько путей обхода, и тогда

$$P_{\text{СЗИ}} = \min\{(1 - P_{\text{НР}}), (1 - P_{\text{обх}1}), \ldots, (1 - P_{\text{обх}k})\},$$

где k — число путей обхода.

Для случая, когда нарушителей более одного и они действуют одновременно по каждому пути, это выражение с учетом совместимости событий будет представлять собой произведение вероятностей

$$P_{\text{СЗИ}} = (1 - P_{\text{НР}})(1 - P_{\text{обх}1})(1 - P_{\text{обх}2}) \cdot \ldots \cdot (1 - P_{\text{обх}k}).$$

Иными словами, в этом случае прочность преграды будет определяться произведением вычетов из единицы значений вероятностей доступа нарушителей к предмету защиты по каждому возможному пути преодоления этой преграды.

Значения $P_{\text{обх}i}$ определяются в диапазоне от 0 до 1 экспертным путем на основе опыта специалистов. В целях унификации метода за основу принимаются следующие градации значений:

$P = 0$ — событие невозможно;
$P = 0{,}2$ — событие маловероятно;
$P = 0{,}5$ — событие вероятно наполовину;
$P = 0{,}8$ — событие вполне вероятно;
$P = 0{,}95$ — вероятность события высокая;
$P = 1$ — событие произойдет наверняка.

Выражение для определения *прочности многозвенной защиты при противостоянии одному нарушителю* может быть представлено в следующем виде:

$$P_{\text{ЗИ}} = \min \left\{ \begin{matrix} P_{\text{СЗИ}1}, P_{\text{СЗИ}2}, \ldots, P_{\text{СЗИ}i}, \\ (1 - P_{\text{обх}1}), (1 - P_{\text{обх}2}), \ldots, (1 - P_{\text{обх}k}) \end{matrix} \right\},$$

где $P_{\text{СЗИ}i}$ — прочность i-й преграды; $P_{\text{обх}k}$ — вероятность обхода преграды по k-му пути.

Выражение для определения *прочности многозвенной защиты при противостоянии группе нарушителей* с учетом совместимости событий может быть представлено в следующем виде:

$$P_{\text{ЗИ}} = P_{\text{СЗИ}1} P_{\text{СЗИ}2} \cdot \ldots \cdot P_{\text{СЗИ}i} (1 - P_{\text{обх}1})(1 - P_{\text{обх}2}) \cdot \ldots \cdot (1 - P_{\text{обх}k}).$$

Из рассмотренного метода определения прочности оболочки защиты можно сделать следующие выводы.

Во-первых, если прочность слабейшего звена защиты удовлетворяет предъявленным требованиям оболочки защиты в целом, возникает вопрос об избыточности прочности на остальных звеньях данной оболочки. Отсюда следует, что экономически целесообразно применять в многозвенной оболочке защиты равнопрочные преграды.

Во-вторых, если звено защиты не удовлетворяет предъявленным требованиям, преграду в этом звене следует заменить на более прочную или дублировать ее еще одной или несколькими преградами. Заметим, что в этом случае все дополнительные преграды должны перекрывать то же число возможных каналов несанкционированного доступа, что и первая преграда. Соответственно, если обозначить прочность дублирующих преград P_1, P_2, P_3, ..., то вероятность преодоления каждой из них нарушителем будет определена как

$$(1 - P_1), (1 - P_2), (1 - P_3), \ldots .$$

В-третьих, считая, что факты преодоления дублирующих преград нарушителем события совместимые, выражение для определения суммарной вероятности преодоления группы дублирующих преград может быть представлено в виде

$$P_{НР} = (1 - P_1)(1 - P_2)(1 - P_3)\cdot \ldots .$$

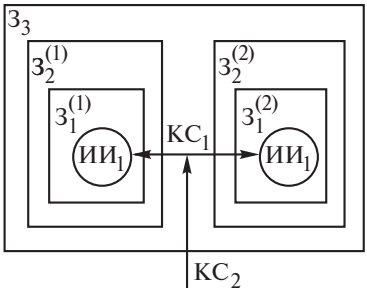


Рис. 6.2. Пример построения оболочек для двух объектов информатизации с использованием одного общего контура

Один из основных принципов построения системы защиты объекта информатизации — необходимость выстраивания вокруг объекта защиты постоянно действующих замкнутых контуров. Пример построения оболочек для двух объектов информатизации, с использованием одного общего контура приведен на рис. 6.2.

Пусть $P_{угр}$ — вероятность возникновения угрозы.

Вероятность того, что все зоны защиты эффективно функционируют, равна

$$P_{защ} = \prod_{i=1}^{n} P_{зi} P_{уязв} = 1 - P_{защ}.$$

Вероятность того, что произошел несанкционированный доступ (НСД) к объекту информатизации, равна

$$P_{НСД} = P_{угр} \prod_{i=1}^{n} (1 - P_{зi}).$$

Точность расчета зависит от точности исходных данных.

Для получения вероятностей проявления отдельных угроз необходимо иметь статистику (закон распределения соответствующих событий). Наиболее распространен экспоненциальный закон распределения.

Выраженная по этому закону вероятность проявления угрозы y_i, равна $P_{yi}(t) = 1 - e^{-\lambda_i t}$, где λ — интенсивность НСД (относительное число НСД в единицу времени).

Если $\lambda_i \ll 1$, то $P_{yi}(t) \approx \lambda_i t$.

6.2. Задания для определения прочности оболочек защиты

1. Элементарные случайные события:

$А^{(2)}$ — нарушитель разрушил защиту в $З_1^{(2)}$,
$В^{(1)}$ — нарушитель разрушил защиту в $З_2^{(1)}$,
$В^{(2)}$ — нарушитель разрушил защиту в $З_2^{(2)}$,
С — нарушитель разрушил защиту в $З_3$,
$Д^{(1)}$ — нарушитель получил НСД к $ИИ_1$ через $КС_1$,
$Д^{(2)}$ — нарушитель получил НСД к $ИИ_2$ через $КС_1$,
Е — нарушитель получил НСД к $ИИ_1$ и $ИИ_2$ через $КС_2$.

2. Интенсивности наступления перечисленных в п. 1 событий λ приведены в табл. 6.1.

Таблица 6.1

Варианты интенсивности наступления событий

Вариант	$\lambda\{А^{(1)}\}$	$\lambda\{А^{(2)}\}$	$\lambda\{В^{(1)}\}$	$\lambda\{В^{(2)}\}$	$\lambda\{С\}$	$\lambda\{Д^{(1)}\}$	$\lambda\{Д^{(2)}\}$	$\lambda\{Е\}$
	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*
1	0,0007	0,0007	0,0025	0,0001	0,00295	0,0005	0,00385	0,00325
2	0,0006	0,0004	0,0045	0,0002	0,00285	0,0007	0,00455	0,00255
3	0,0008	0,0005	0,0015	0,0004	0,00325	0,0008	0,00556	0,00225
4	0,0125	0,0002	0,0025	0,0001	0,00355	0,0005	0,00425	0,00225
5	0,0005	0,0005	0,0015	0,0001	0,00025	0,0005	0,00225	0,00456

3. Подсчитать вероятности событий 1–8 при $T = 500$ ч.

4. Найти вероятности сложных событий:

$$P\{Д^{(1)} + Е\} = P\{Д^{(1)}\} + P\{Е\} - P\{Д^{(1)}\}P\{Е\},$$

$$P\{Д^{(2)} + Е\} = P\{Д^{(2)}\} + P\{Е\} - P\{Д^{(2)}\}P\{Е\},$$

$$P\{\text{CB}^{(1)}\cdot\text{A}^{(1)}\} = P\{\text{C}\}P\{\text{B}^{(1)}\}P\{\text{A}^{(1)}\},$$

$$P\{\text{CB}^{(2)}\cdot\text{A}^{(2)}\} = P\{\text{C}\}P\{\text{B}^{(2)}\}P\{\text{A}^{(2)}\},$$

$$P\{\text{CB}^{(1)}\cdot\text{A}^{(1)} + \text{CB}^{(2)}\cdot\text{A}^{(2)}\} = 1 - (1 - P\{\text{CB}^{(1)}\cdot\text{A}^{(1)}\})(1 - P\{\text{CB}^{(2)}\cdot\text{A}^{(2)}\}),$$

$$P\{\text{E} + \text{CB}^{(1)}\cdot\text{A}^{(1)} + \text{CB}^{(2)}\cdot\text{A}^{(2)}\} = \\ = 1 - (1 - P\{\text{E}\})(1 - P\{\text{CB}^{(1)}\cdot\text{A}^{(1)}\})(1 - P\{\text{CB}^{(2)}\cdot\text{A}^{(2)}\}).$$

5. Построить график изменения вероятности $P\{\text{E} + \text{CB}^{(1)}\cdot\text{A}^{(1)} + \text{CB}^{(2)}\cdot\text{A}^{(2)}\}$ от времени при $T = (0...1000)$ ч.

6. Уменьшить наибольшую интенсивность в 4 раза и посмотреть, как это повлияло на изменение вероятности $P\{\text{E} + \text{CB}^{(1)}\cdot\text{A}^{(1)} + \text{CB}^{(2)}\cdot\text{A}^{(2)}\}$ от времени (построить график).

7. Определить, во сколько раз требуется уменьшить все интенсивности, чтобы вероятность $P\{\text{E} + \text{CB}^{(1)}\cdot\text{A}^{(1)} + \text{CB}^{(2)}\cdot\text{A}^{(2)}\}$ уменьшилась в 2 раза при неизменном значении времени.

8. Представить в отчете вычисления и графики. Сделать выводы по проделанной работе.

Контрольные вопросы и задания

1. В чем заключается сложность функционального построения системы защиты объекта информатизации? Приведите примеры.
2. Приведите формулу для вычисления величины $P_{\text{отк}}(t)$, прокомментируйте ее.
3. Приведите примеры многозвенной системы защиты объекта информатизации.
4. Прокомментируйте выражение для определения прочности многозвенной защиты при противостоянии одному нарушителю.
5. Прокомментируйте выражение для определения прочности многозвенной защиты при противостоянии нескольким нарушителю.
6. Какие выводы можно сделать, если прочность слабейшего звена защиты удовлетворяет предъявленным требованиям оболочки защиты в целом?
7. Какие меры повышения прочности защиты можно порекомендовать, если звено защиты не удовлетворяет предъявленным требованиям?

СПИСОК ЛИТЕРАТУРЫ

1. *Бабаш А.В.*, *Баранова Е.К.* Информационная безопасность: Учеб.-практ. пособие. — М.: Изд. Центр ЕАОИ, 2010. — 376 с.
2. *Баранова Е.К.*, *Бабаш А.В.* Информационная безопасность и защита информации. — М.: РИОР: ИНФРА-М, 2013. — 256 с.
3. *Баранова Е.К.* Методики и программное обеспечение для оценки рисков в сфере информационной безопасности // Управление риском. — 2009. — № 1 (49). — С. 15–26.
4. *Малюк А.А.* Информационная безопасность: концептуальные и методологические основы защиты информации: Учеб. пособие для вузов. — М.: Горячая линия — Телеком, 2004. — 280 с.
5. *Петренко С.А.*, *Симонов С.В.* Управление информационными рисками. Экономически оправданная безопасность. — М.: Компания АйТи: ДМК Пресс, 2004. — 384 с.
6. *Шумский А.А.*, *Шелупанов А.А.* Системный анализ в защите информации: Учеб. пособие для студентов вузов. — М.: Гелиос АРВ, 2005. — 224 с.
7. *Bjorn A.G.* (January 2002). CORAS, A Platform for Risk Analysis on Security Critical Systems — Model-based Risk Analysis Targeting Security. — URL: www.nr.no/coras
8. Методика оценки рисков с использованием программного комплекса ГРИФ. — URL: http://citforum.ru/products/dsec/grif/
9. ГРИФ — программный комплекс для анализа и контроля рисков информационных систем компаний. — URL: http://www.sec4all.net/grif.html
10. Сети Петри для моделирования дискретных систем. — URL: http://itmu.vsuet.ru/Subjects/Matmodel-pk/Seti-Petri.htm

ПРИЛОЖЕНИЕ 1

Варианты заданий

ВАРИАНТ 1

Структура малого предприятия и схема с указанием перечня помещений и оборудования, используемого для обработки защищаемой информации.

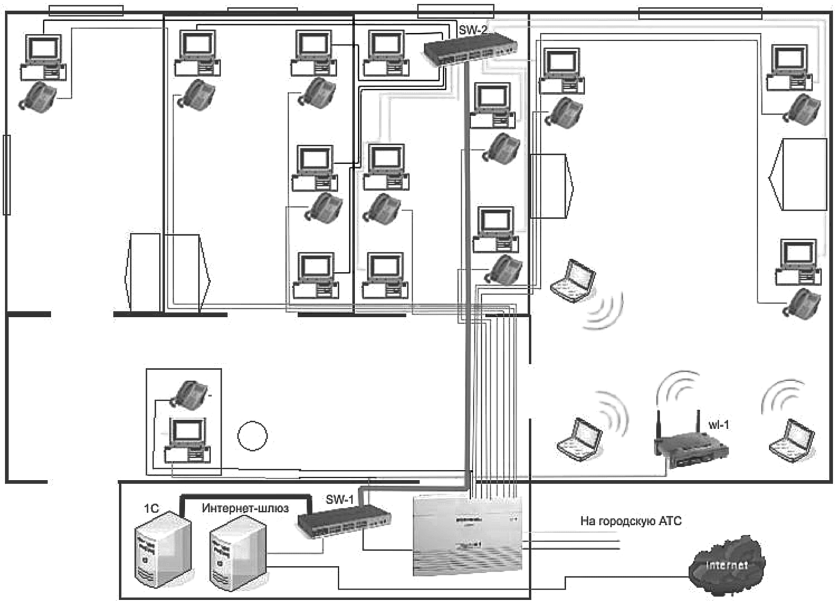


Рис. П1.1. Схема объекта информатизации

На этой схеме представлена главная офисная сеть компании «АСС-инжиниринг». Компания предоставляет профессиональные услуги по проектированию и комплексному оснащению различных объектов инженерными системами, включая монтаж, пусконаладку и интеграцию систем внутреннего электроснабжения и освещения,

вентиляции и кондиционирования, учета расхода тепловодопотребления, систем безопасности, телефонной связи, структурированных и телерадиовещательных сетей, объединенных в единую систему жизнедеятельности здания. Также компания осуществляет гарантийное и сервисное обслуживание созданных систем и обучение персонала заказчика. Следовательно, возникает проблема защиты коммерческой и служебной информации.

У компании есть ряд помещений и складов, с которыми требуется поддерживать рабочую связь. Выдвигается на первый план проблема обмена информацией между ними по телефону и через Интернет.

Объект представляет собой помещение из шести комнат: коридор (секретарь); серверная; кабинет директора (переговорная); бухгалтерия; расчетный отдел; проектный отдел.

Для обработки защищаемой информации используется 13 компьютеров и 3 ноутбука.

Сеть разделена на три группы при помощи управляемых коммутаторов 2-го уровня с поддержкой *vlan*. Первая группа имеет доступ к серверу 1С, к общим ресурсам компьютеров, входящих в группу, и выход в Интернет. Вторая группа имеет доступ к серверу 1С, не имеет доступа к компьютерам остальных групп и выхода в Интернет. Третья группа — это ноутбуки, подключенные по беспроводной сети (wi-fi) через точку доступа *wl-1*, и имеющие доступ только к Интернету.

Также имеется мини-АТС, подключенная к внешним городским линиям и к интернет для использования ip-телефонии.

ВАРИАНТ 2

1. План предприятия и назначение помещений

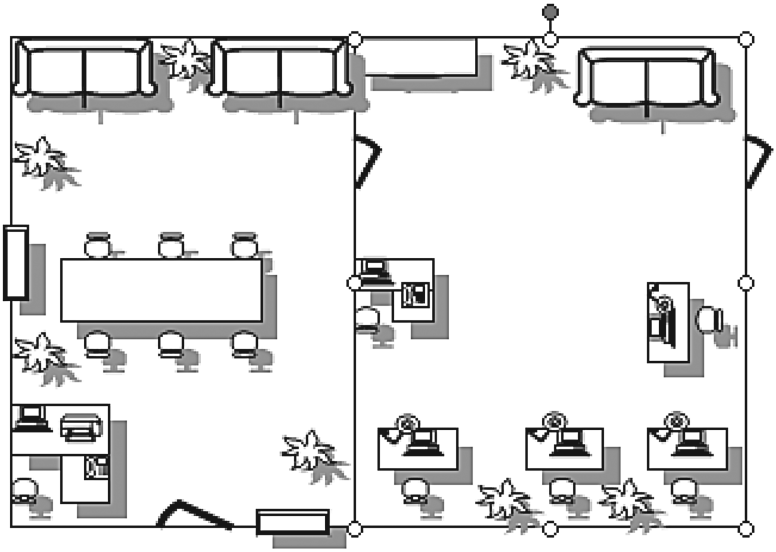


Рис. П1.2. Схема объекта информатизации

Объект оценки представляет собой помещение из двух комнат, одна из которых является приемной и служит также для ведения переговоров, а другая используется для выполнения заказов в области разработки комплексных систем безопасности информации. Находящаяся в данном помещении организация занимается выполнением контрактов в информационной сфере (разработкой ЛВС, систем безопасности, созданием корпоративных сетей и т.п.). Для обработки защищаемой информации используется несколько компьютеров, находящихся в помещении без окон. Есть телефон, хранилище документов, сотрудники имеют возможность переговариваться во время работы. Сеть основана на оптоволокне, выхода в Интернет нет. Помещения предприятия находятся под охраной. Вход в помещение для переговоров возможен из коридора и из помещения, в котором выполняются заказы (операторской), вход же в операторскую возможен из помещения для переговоров и коридора. Коридоров два, они связаны между собой. Все двери стальные, оснащены замками и доводчиками.

2. Перечень информации, циркулирующей на предприятии

Вид информации	*Возможные потери*, руб.*
Плановая документация	80 000
Информационно-справочная и справочно-аналитическая документация	80 000
Отчетная документация	120 000
Документация по обеспечению кадрами	30 000
Финансовая документация	1 000 000
Материально-техническое снабжение	200 000
Договорная документация	200 000
Информация по заказчикам (а также по выполненным заказам)	1 200 000
Информация по новым разработкам	500 000

* Возможные потери определены по данным предприятия.

3. Параметры локальной сети и список сотрудников

Параметры локальной сети:
– число компьютеров — 6;
– сеть построена на оптоволокне.

Персонал состоит из *постоянного* и *переменного состава*:
– *Постоянный состав*:
  1) генеральный директор;
  2) заместитель директора;
  3) секретарь;
  4) юрист;
  5) бухгалтер;
  6) администратор сети и безопасности;
  7) программист;
  8) сотрудники-специалисты в области безопасности — 5 чел.;
  9) сотрудники охраны— 2 чел.;
  10) уборщица.
– *Переменный состав*:
  1) заказчики
  2) доверенные лица заказчиков.

4. Перечень угроз с учетом возможных потерь

Угроза	*Объект угрозы*	*Опасность угрозы в баллах от 1 до 100*	*Возможные потери, руб.*
Визуальный съем информации	Различная информация	10 (вся защищаемая информация обрабатывается в помещении без окон)	10 000
Лазерный съем акустической информации с окон	Секретные переговоры	30	100 000
Съем информации за счет ПЭМИН	Различная информация	60	40 000
Радио-закладки в стенах и в мебели	Секретные переговоры	50	90 000
Съем информации с телефонной линии	Секретная информация, устные договоренности с заказчиками	60	120 000
Утечки информации за счет персонала (внутренние угрозы)	Вся информация	80	250 000
НСД с проникновением в помещение	То же	60	300 000
Пожар	Различная информация (за исключением документированной информации, хранимой в огнеупорном сейфе)	40	500 000
Вредоносные программы	Информация локальной сети	40	100 000
Хищение носителей информации	Различная информация	50	90 000
Визуальный съем с дисплея и принтера	То же	20	Незначительные
Производственные и технологические отходы	Служебная и профессиональная тайны	20	То же
Утечка по цепям заземления	Различная информация	20	–II–
Съем информации по системе вентиляции	Разговоры	40	–II–

ВАРИАНТ 3

1. Описание структуры предприятия

Объект оценки представляет собой помещение из трех комнат: приемная, рабочая комната основного персонала и кабинет директора. Организация, расположенная в данном помещении, занимается закупкой печатной и канцелярской продукции у производителя и последующим распространением по книжным магазинам. Следовательно, возникает проблема защиты коммерческой и служебной информации.

Для обработки защищаемой информации используется 7 компьютеров, 6 из которых расположены в помещении без окон. Вся конфиденциальная информация хранится на сервере, находящемся в

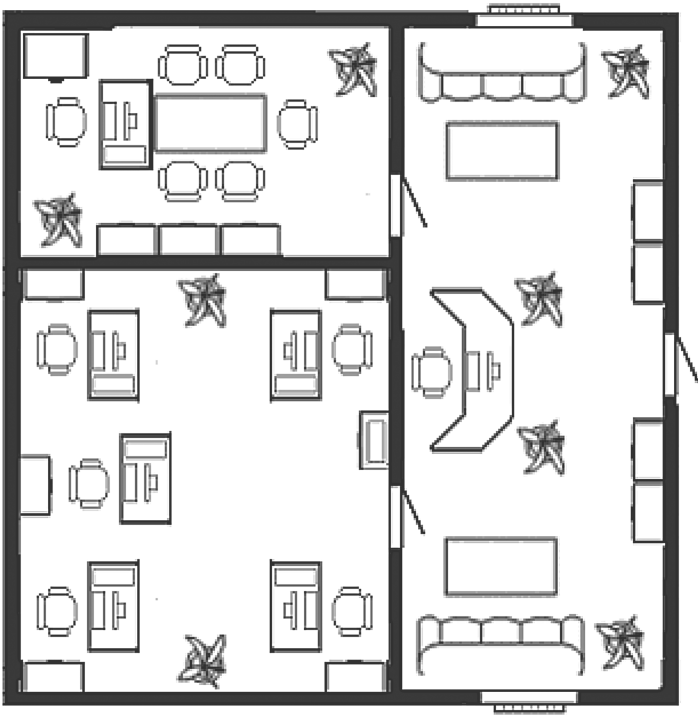


Рис. П1.3. Схема объекта информатизации

закрытом серверном шкафу. Есть телефон, сотрудники имеют возможность переговариваться в процессе работы и совершать внешние звонки. Сеть основана на экранированной витой паре, что исключает возможность снятия информации с кабеля. Сеть имеет доступ в Интернет через прокси-сервер. Защита внутренней сети реализована аппаратно посредством межсетевого экрана маршрутизатора и программно посредством межсетевого экрана, установленного на прокси-сервере. Все конфиденциальные переговоры ведутся в помещении без окон.

Перечень помещений:

1. *кабинет генерального директора*. Постоянное рабочее место директора, в кабинете расположен сейф для хранения конфиденциальных документов и денежной наличности. В кабинете происходят рабочие совещания;

2. *рабочий кабинет сотрудников*. В кабинете расположены 5 рабочих мест постоянных сотрудников, сервер в закрытом серверном шкафу. Посетители в помещение допускаются исключительно под контролем сотрудников;

3. *приемная*. В помещении постоянно работает секретарь. Здесь происходит прием посетителей.

Перечень оборудования:

1. ПК сотрудников — 7 шт.;
2. сервер (включает файл-сервер, прокси-сервер);
3. сетевой маршрутизатор;
4. МФУ;
5. телефоны — 7 шт.;
6. огнеупорный сейф.

2. Анализ угроз

Угроза	*Объект угрозы*	*Способ обнаружения*	*Последствия*	*Способ предотвращения*
Визуальный съем информации	Различная информация (в основном визуальный съем с мониторов)	Обнаруживается при визуальном осмотре прилегающей к помещению территории и света на стекле	Получение злоумышленником важной информации, нарушение ее конфиденциальности	На данном предприятии используются вертикальные жалюзи, расположенные внутри помещения, рабочие места сотрудников расположены в комнатах без окон

Продолжение таблицы

Угроза	*Объект угрозы*	*Способ обнаружения*	*Последствия*	*Способ предотвращения*
Съем информации за счет ПЭМИН	Угрожает объектам, подверженным ПЭМИН (система противопожарной и охранной сигнализации, наводки на некоторые элементы ПК и систем передачи по каналам)	Обнаруживается с помощью системы мониторинга	Может осуществляться съем информации, обрабатываемой этим устройством, нарушение ее конфиденциальности	Установка генератора пространственного зашумления
Съем информации с телефонной линии	Телефоны, телефонные линии	Обнаруживается при контроле напряжения телефонной линии	Получение конфиденциальной информации, устных договоренностей с клиентами, информации о поставщиках и клиентах	Установка устройств контроля напряжения телефонной линии
Утечки информации за счет персонала (внутренние угрозы)	Вся информация	Организационные меры контроля за деятельностью сотрудников	Разглашение конфиденциальной информации, потеря деловой репутации и т.п.	Предотвращается организационными методами, правильной мотивацией сотрудников, разграничением доступа к информации
НСД с проникновением в помещение или в локальную сеть	Вся информация, все технические средства предприятия	Охранная сигнализация, анализ межсетевого экрана	НСД к информации, нарушение системы защиты, установка радиозакладок и т.п.	Помещение: установка внешней стальной двери, замков на внутренних дверях, система охранной сигнализации, охрана здания КПП на входе, в котором расположен офис предприятия. Сеть: на прокси-сервере установлен межсетевой экран

Окончание таблицы

Угроза	*Объект угрозы*	*Способ обнаружения*	*Последствия*	*Способ предотвращения*
Радиозакладки в стенах и в мебели	Речевая информация, секретные переговоры	Обнаруживается спецустройствами, которые выявляют радиосигналы таких закладок	Компрометация фирмы, получение информации о заказчиках, выполнении заказов и внутреннего положения дел предприятия	Установка устройства противодействия радиоэлектронным средствам промышленного шпионажа и защита телефонной линии от жучков и подслушивающих устройств
Потеря информации из-за вирусов	Вся информация, обрабатываемая и хранимая на ПК и сервере. Частота появления высока	Обнаруживается при наличии антивирусных программ	Приводит к нарушению доступности и целостности информации. Может привести к утрате всей информации и нарушению функционирования оборудования	Предотвращается организационными мерами и установкой лицензионного ПО, постоянно обновляемого антивируса, межсетевого экрана (прокси-сервер)
Потеря или съем информации из-за шпионских программ	Вся информация, обрабатываемая и хранимая на ПК и сервере	Обнаруживается при наличии антишпионского ПО его реакцией, нестандартным поведением ПО	Приводит к нарушению доступности, целостности, конфиденциальности информации. Может привести к утрате всей информации и нарушению функционирования оборудования	Предотвращается организационными мерами и установкой антишпионского ПО
Пожар	Вся информация (кроме хранимой в огнеупорном сейфе), а также техническое оснащение и офисная мебель	Визуальный и при помощи противопожарной системы	Потеря информации, оборудования, остановка деятельности предприятия, простой в работе	Система противопожарной сигнализации, план эвакуации при пожаре, огнетушители, огнеупорный сейф

ВАРИАНТ 4

Защищаемый объект информатизации находится в здании головного офиса Интернет-магазина компании «Мистэри» на первом этаже здания, предоставляющей свои услуги в области книжной и канцелярской продукции, игр и игрушек, аудио- и видео-дисков, а также иных товаров.

Описание объекта информатизации

Характеристика	*Описание*
Название ОИ	Серверная комната ЗАО «Мистэри»
Режим обработки информации	Многопользовательский режим обработки информации с разным уровнем доступа
Класс АС	1Г (в соответствии с руководящими документами ФСТЭК)
Количество субъектов доступа	Физический доступ в серверную — 1 чел., доступ к данным на серверах — 150 сотрудников компании
Категория обрабатываемой информации	• информация открытого характера; • персональные данные (ПД) сотрудников; • коммерческая тайна
Тип системы	Распределенная (есть связи с филиалами и возможность удаленного доступа к сети и данным на ОИ для сотрудников компании)

Сбор клиентских сведений, относящихся к ПД, осуществляется через веб-сайт компании, дальнейшая их обработка производится на сервере БД.

В серверной комнате ЗАО «Мистери» расположены 2 сервера (сервер БД и сервер сайта компании). На обоих выполняются сбор, обработка и хранение ПД. Более подробная информация представлена в документе.

На объекте используются следующие меры по защите информации:

1. Окна и двери тщательно герметизированы монтажной пеной.
2. Окна защищены от лазерной прослушки рифлением.
3. Весь персонал нанят по договору с применением пункта, гарантирующим сохранение персональных данных и коммерческой тайны.
4. Парольная защита на ресурсы.
5. Помещения оборудованы системами охранной сигнализации, вход в серверную комнату осуществляется с использованием смарт-карт.

6. Система видеонаблюдения.

7. Между помещениями стоят деревянные двери, во внешние помещения ведет стальная дверь.

8. Используется лицензионное ПО.

9. Все помещения оборудованы системами противопожарной сигнализации.

РВС организации оборудована криптомаршрутизатором для организации защищенного VPN-соединения с пунктом выдачи заказов и маршрутизатором со встроенным концентратором для идентификации и аутентификации сотрудников по IP-адресам.

Рис. П1.4. Схема объекта информатизации. План контролируемой зоны

ВАРИАНТ 5

Офис компании ООО «Диджитал Коммерц» представляет собой помещение из четырех комнат: приемная, серверная, кабинет № 101 (кабинет директора) и кабинет № 102 (кабинет сотрудников). Офис расположен на 4-м этаже 8-этажного офисного здания, представляющего собой современное стекложелезобетонное строение. В этом офисном здании расположено 12 компаний, 2 из них (включая ООО «Диджитал Коммерц») — на 4-м этаже.

Описание объекта оценки

Характеристика	*Описание*
Название ОИ	Информационная система электронной коммерции
Режим обработки информации	Многопользовательский режим обработки информации с разным уровнем доступа
Класс АС	1Г
Число субъектов доступа	6 чел.
Категория информации	Коммерческая тайна, персональные данные (К3)
Тип сетевой структуры	Локальная вычислительная сеть с выходом в Интернет и удаленным доступом к ее ресурсам
Состав АС	6 рабочих станций и 1 сервер

Возникает проблема защиты коммерческой информации и персональных данных клиентов и сотрудников компании.

Для обработки защищаемой информации используется несколько компьютеров, все они находятся в помещении с окнами. В приемной, кабинетах № 101 и 102 есть внутренний телефон с «выходом в городскую АТС», хранилище бумажных документов находится в кабинете № 101. Проводная сеть основана на экранированной витой паре 5-й категории, что значительно уменьшает возможность снятия информации с кабеля. Выход в Интернет осуществляется через маршрутизатор с сетевым экраном и поддержкой NAT, VPN. Каждому сотруднику выдается постоянный электронный пропуск (смарт-карта) с фотографией, посетителям выдается временный пропуск. Пропуск предоставляет вход в офис, доступ в серверную комнату предоставляется только директору и системному администратору при помощи смарт-карты.

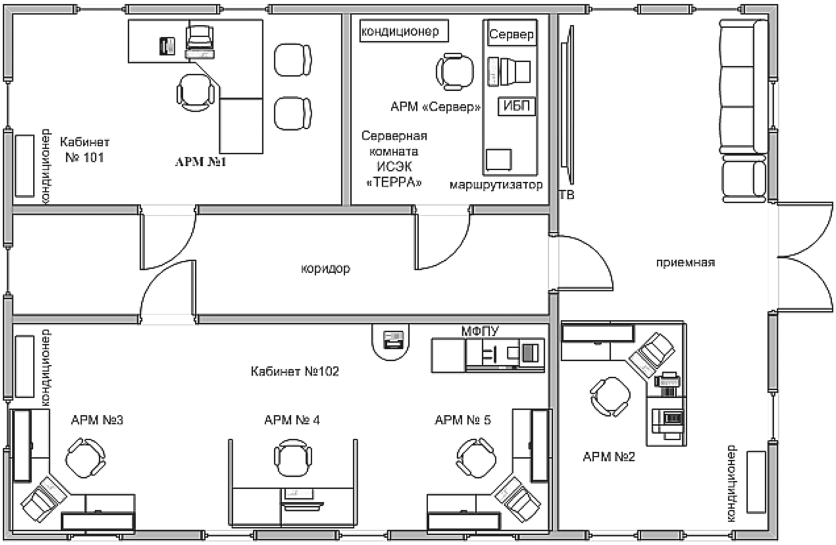


Рис. П1.5. Схема объекта информатизации. План контролируемой зоны

На объекте используются следующие меры защиты информации:

1. Окна и двери тщательно герметизированы монтажной пеной.
2. Окна защищены от оптической разведки при помощи шторжалюзи.
3. Весь персонал нанят по договору с применением пункта, гарантирующего сохранение персональных данных и коммерческой тайны.
4. Парольная защита на ресурсы.
5. Помещения оборудованы системами охранной сигнализации, вход в серверную комнату осуществляется с использованием смарт-карт.
6. Система видеонаблюдения.
7. Между помещениями стоят деревянные двери, во внешние помещения и в серверную комнату ведут стальные двери с электронным замком (доступ по смарт-картам).
8. Используется лицензионное ПО.
9. Все помещения оборудованы системами противопожарной сигнализации.

10. ЛВС организации имеет доступ в глобальную сеть через маршрутизатор со встроенным сетевым экраном, дополнительно используется технология NAT (для сокрытия внутренних адресов и структуры ЛВС) и VPN (для работы с клиентами по защищенным каналам).

11. Система ИСЭК (ЛВС) аттестована в соответствие с РД ФСТЭК на класс АС-1Г, а как информационная система обработки персональных данных — на класс К3.

ПРИЛОЖЕНИЕ 2

Пример выполнения работы по анализу рисков информационной безопасности с использованием программы CORAS

ВАРИАНТ 3

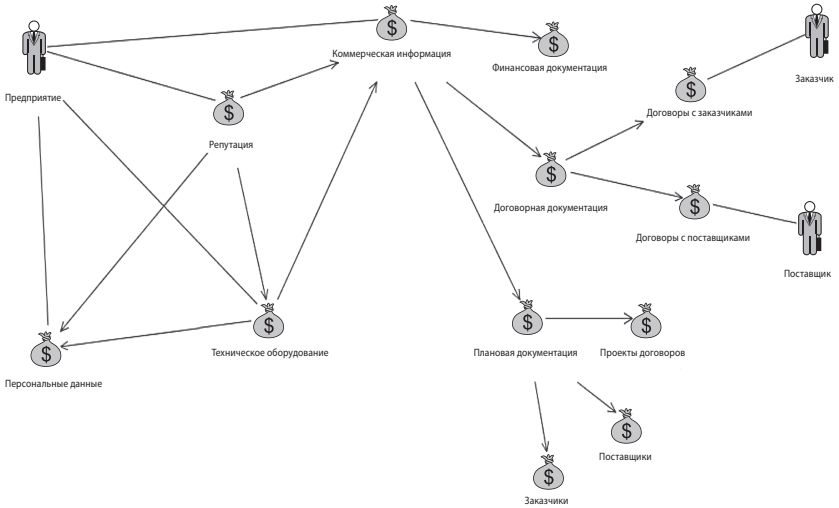


Рис. П2.1. Диаграмма активов

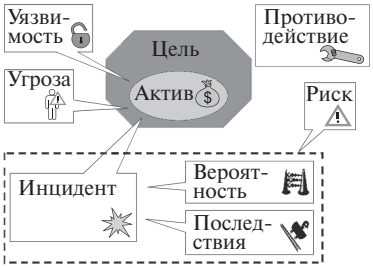


Рис. П2.2. Элементы анализа

Элементы анализа можно представить в виде схемы рис. П2.2:

Составим табл. П2.1 для полного описания модели рисков с использованием информации по защите объекта. В ней также приведена параллель между объектами программного обеспечения и традиционными вопросами для анализа рисков.

Таблица П2.1

Риски

Кто/что причина?	*Как? Какой инцидент? Чему угрожает?*	*В связи с чем стала возможной уязвимость*
Нарушитель	Хищение информации с сервера	Отсутствие шифрования
		Незащищенность от НСД из внешней среды
	Несанкционированное копирование информации	Ошибки в разграничении доступа
		Простой пароль
	Визуальный съем информации	Небрежное хранение документации
	Хищение аппаратуры, материальных носителей	Возможность доступа к охранным системам
	Съем информации за счет ПЭМИН	Возможность подключения к устройствам
	Запись речевой информации с помощью диктофона, радио-закладок	Отсутствие наблюдения за посетителями и проверок на наличие таких устройств
Системные сбои	Потеря информации	Отсутствие копии
Вирус, закладки	Потеря информации	Ошибки пользователей
		Установка своего ПО
		Посещение вредоносных сайтов
Персонал	Хищение материальных носителей	Небрежное хранение документации
		Трудовой договор
	Копирование информации на носители	Простой пароль
		Политика безопасности
	Доступ к защищаемой информации	Ошибки администратора
Пожар	Уничтожение технического оборудования	Сбои в работе пожарной сигнализации
	Уничтожение материальных носителей	

Составим матрицу рисков, в которой столбцы являются шкалой последствий нежелательных инцидентов, а строки — вероятностью происхождения данного инцидента, или его частоты (табл. П2.2).

Таблица П2.2

Матрица рисков

		Шкала последствий нежелательных инцидентов			
		Незначительные	*Минимальные*	*Средние*	*Катастрофические*
Вероятностная шкала	*Редко*	Приемлемый	Приемлемый	Приемлемый	Неприемлемый
	Иногда	Приемлемый	Приемлемый	Неприемлемый	Неприемлемый
	Регулярно	Приемлемый	Неприемлемый	Неприемлемый	Неприемлемый
	Часто	Неприемлемый	Неприемлемый	Неприемлемый	Неприемлемый

Используя табл. П2.1, строим модели угроз (рис. П2.3– П2.4).

Генерируем диаграмму рисков (щелкаем правой кнопкой мыши по вкладке *Угрозы* и выбираем *Generate risk diagram*), далее по каждому риску для каждого актива определяем последствия в случае осуществления этого риска. Полученная диаграмма представлена на рис. П2.5.

В соответствии с рис. П2.6, занесем полученную информацию в матрицу рисков, получим следующую табл. П2.3.

Таблица П2.3

Матрица рисков по диаграмме

		Шкала последствий нежелательных инцидентов			
		Незначительные	*Минимальные*	*Средние*	*Катастрофические*
Вероятностная шкала	*Редко*			Переманивание клиентов. Изменение коммерческой информации. Изменение ПДн. Удаление ПДн	Хищение коммерческой информации. Удаление коммерческой информации. Хищение ПДн. Поломка/уничтожение технического оборудования
	Иногда			Копирование коммерческой информации. Копирование ПДн	
	Регулярно				
	Часто				

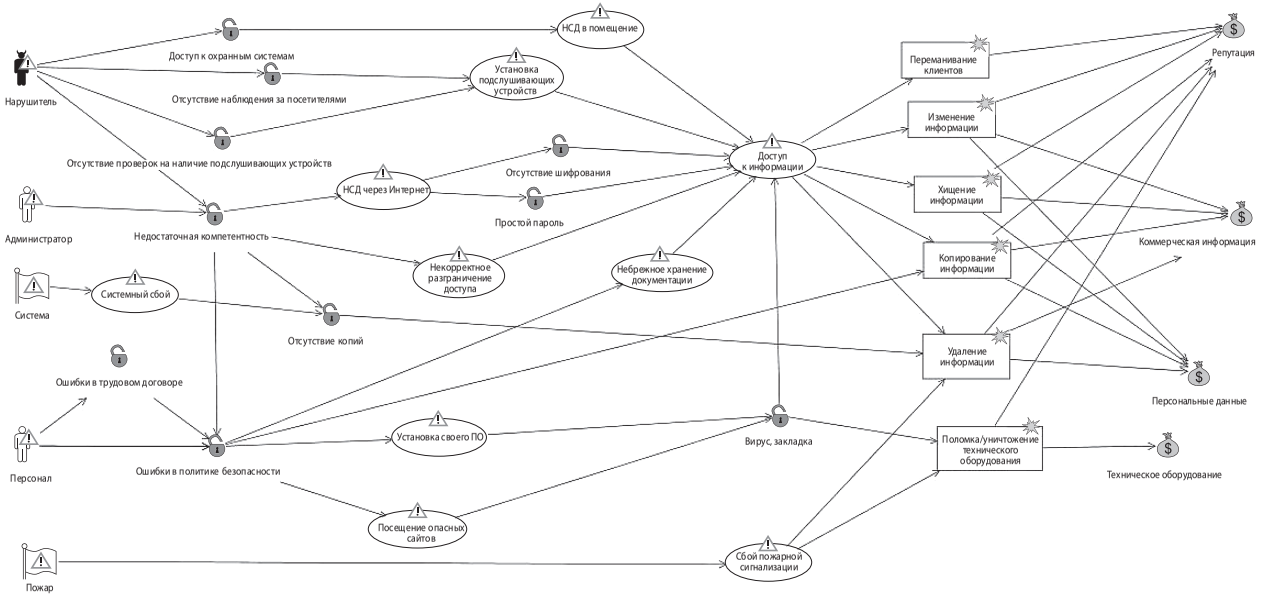


Рис. П2.3. Модель угроз

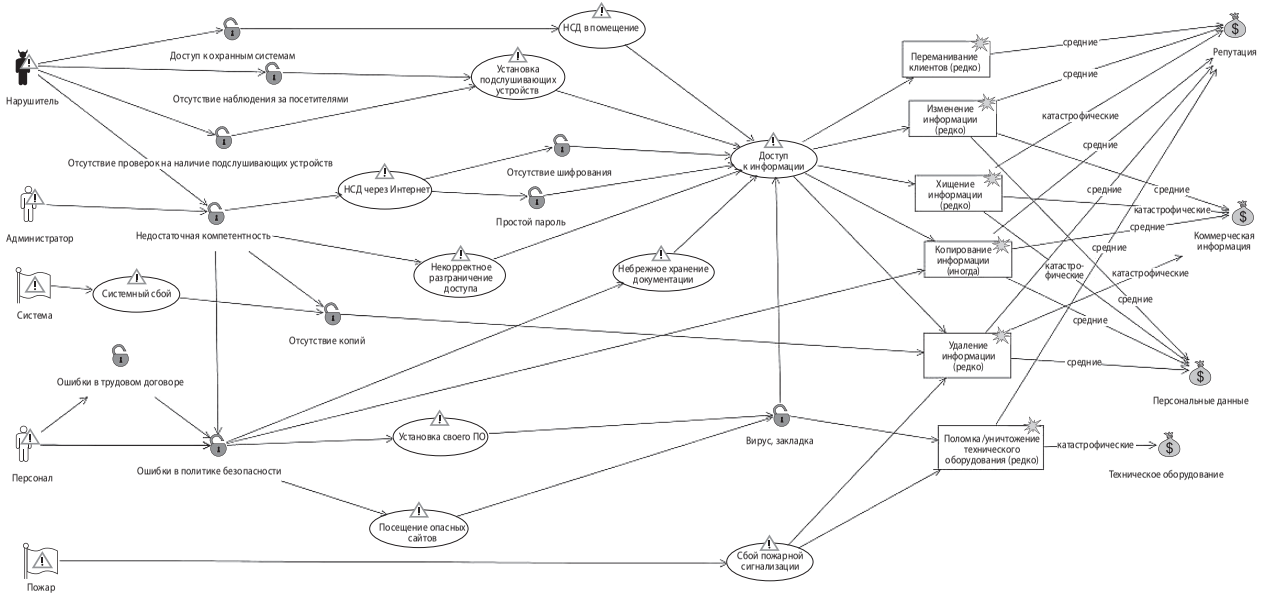


Рис. П2.4. Модель угроз с вероятностными характеристиками

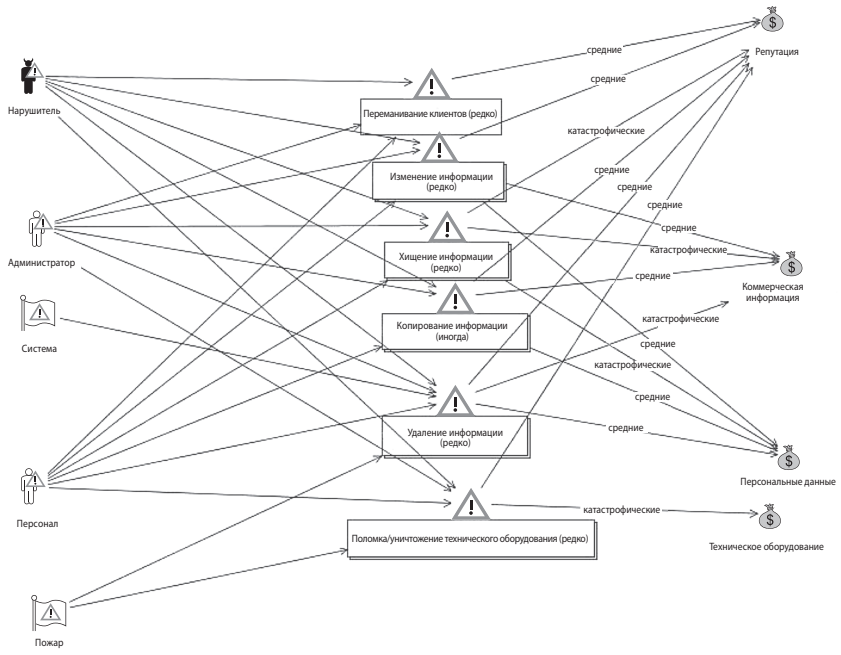


Рис. П2.5. Диаграмма рисков с характеристикой последствий осуществления угрозы

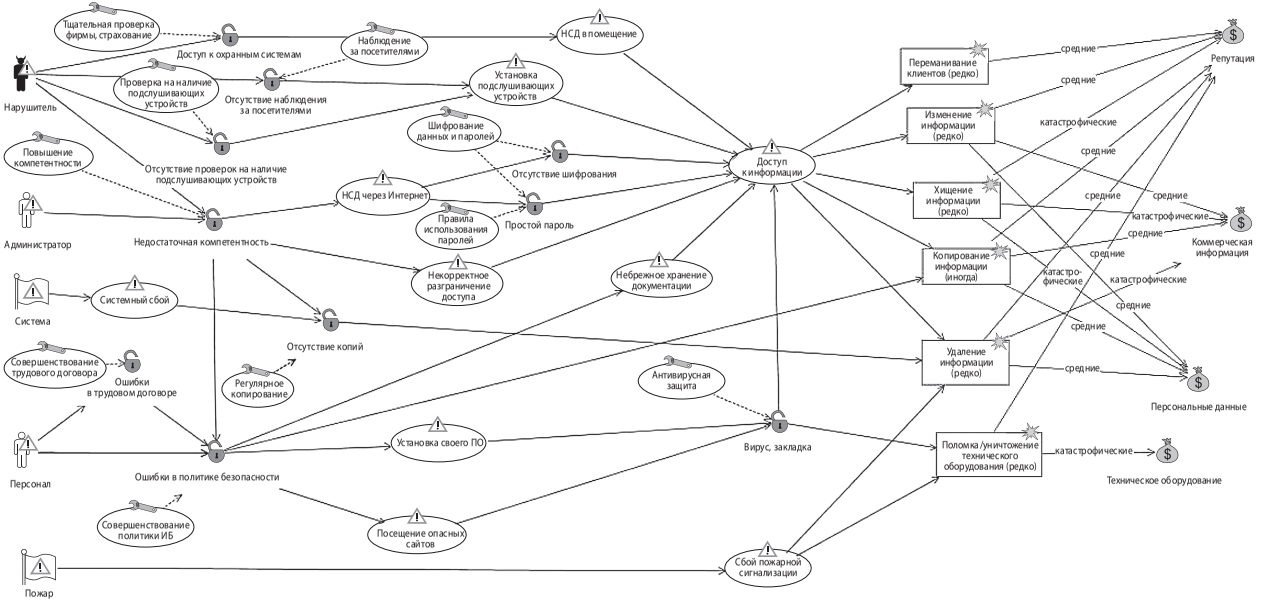


Рис. П2.6. Диаграмма угроз после добавления противодействий

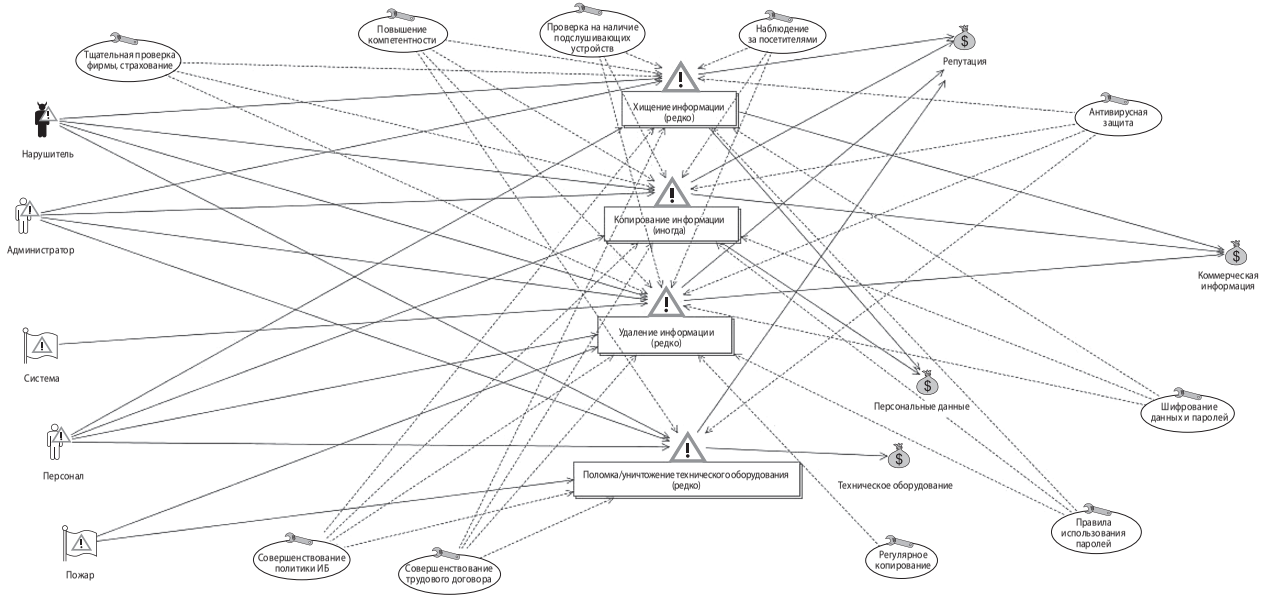


Рис. П2.7. Диаграмма неприемлемых рисков

Выводы

На основании диаграммы неприемлемых рисков (рис. П2.7) можно предложить следующие противодействия в порядке влияния на риски:

- Повышение квалификации администратора.
- Совершенствование политики информационной безопасности.
- Хранение данных на сервере в зашифрованном виде.
- Создание сложных паролей и их хранение их в зашифрованном виде.
- Регулярное копирование информации.
- Включение в трудовой договоров пунктов о неразглашении коммерческой информации, регламентирование обязанностей сотрудника.
- Регулярное обновление и настройка антивирусного ПО.
- Наблюдение за посетителями.
- Проверка на наличие подслушивающих устройств.
- Использование лицензионного программного обеспечения. Все ПО устанавливается под контролем и от имени администратора. Любая попытка установить собственное ПО мгновенно обнаруживается и фиксируется в журнале.
- Обучение персонала, разработка организационных мер защиты информации, строгое соблюдение правил политики безопасности.

ПРИЛОЖЕНИЕ 3

Общие сведения о компании

Рассматриваемое общество с ограниченной ответственностью «Перспектива» основано в 2008 г. В компании принят Устав организации, в котором определено, что основными видами ее деятельности являются:

- аутсорсинг;
- разработка сайтов;
- продажа продукции;
- установка технического оборудования;
- ремонт оргтехники и заправка картриджей.

А также при индивидуальных заказах разрабатываются системы защиты предприятия-заказчика для защиты коммерческой тайны.

Организационная структура компании ООО «Перспектива»

Персонал указанной компании состоит из постоянного и переменного состава:

- В постоянный состав входят:
  - директор;
  - заместитель директора по коммерческим вопросам;
  - бухгалтер;
  - секретарь;
  - менеджер по продажам;
  - менеджер по обслуживанию продукции компании 1С;
  - четыре системных администратора.
- Переменный состав представлен уборщицей.

Общее количество сотрудников компании — 11.

В структуре компании рассматриваем следующие подразделения:

- дирекция;
- бухгалтерия;
- секретариат;
- отдел продаж;
- отдел информационных технологий (ИТ).

Основные функции, реализуемые организационно-штатной структурой компании, приведены в табл. П3.1.

Таблица П3.1

Основные функции должностной структуры компании

Должность	Реализуемые функции
Дирекция	Руководство компанией. Разработка комплексной системы защиты. Решение вопросов финансово-экономической деятельности компании
Бухгалтерия	Осуществление расчетов/платежей (наличным путем, безналичным) с юридическими и физическими лицами. Просчет стоимости системы защиты. Выплата зарплаты, пособий, отпускных, иных платежей. Подготовка и сдача отчетности, предусмотренной законодательством РФ
Секретариат	Прием посетителей. Ответ на телефонные звонки и согласование встреч с руководством. Ведение документооборота (регистрация документов, отправление и прием документов). Обеспечение канцелярскими принадлежностями и хозяйственными товарами
Отдел продаж	Осуществление поставки товара на склад. Реализация товара клиентам
Отдел информационных технологий	Аутсорсинг. Установка системы защиты. Обеспечение надлежащей работы компьютерной и организационной техники

Схема организационно-штатной структуры организации и взаимодействие отделов между собой приведена на рис. П3.1.

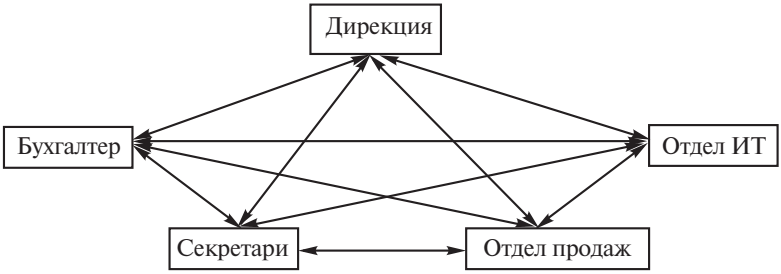


Рис. П3.1. Схема организационно-штатной структуры Компании

Размещение компании

Компания ООО «Перспектива» арендует два офиса в бизнес-центре. Вход в бизнес-центр не ограничен с 9.00 до 20.00 по будням. Ночью территория охраняется сотрудниками вневедомственной охраны. Объект оснащен системой видеонаблюдения, въезд на территорию возможен только через ворота, оснащенные шлагбаумом, только по специальным пропускам, которые выдаются администрацией бизнес-центра.

Все помещения компании ООО «Перспектива» оборудованы механическими замками. Ключи от помещений, кроме серверной комнаты, имеются у каждого сотрудника и выдаются директором под роспись каждому постоянному сотруднику. Уборщица как переменный персонал имеет доступ только к офису, получив ключи на посту охраны в часы проведения уборки помещений.

В табл. П3.2 приведен перечень подразделений компании с указанием мест их размещения.

Таблица П3.2

Размещение сотрудников компании по комнатам

Номер комнаты	Сотрудники	Подразделения
1	Серверная комната	Отдел ИТ
2	Генеральный директор	Дирекция
2	Бухгалтер	Бухгалтерия
3	Секретарь	Секретариат
3	Сотрудники отдела ИТ	Отдел ИТ
3	Менеджер по обслуживании продукции компании 1С	Отдел ИТ
3	Менеджер по продажам	Отдел продаж

На первом этаже находится основной офис, который разделен на две комнаты (рис. П3.2). В комнате К4 располагается директор и его заместитель. Поскольку директор и его заместитель часто отсутствуют по служебным надобностям, за компьютерами может работать бухгалтер. Кабинет директора дополнительно защищен звукоизоляцией от подслушивания разговоров. Также в данном помещении находится сейф, доступ к которому имеет только директор. Секретарь тоже имеет доступ к сейфу, но только в присутствии директора.

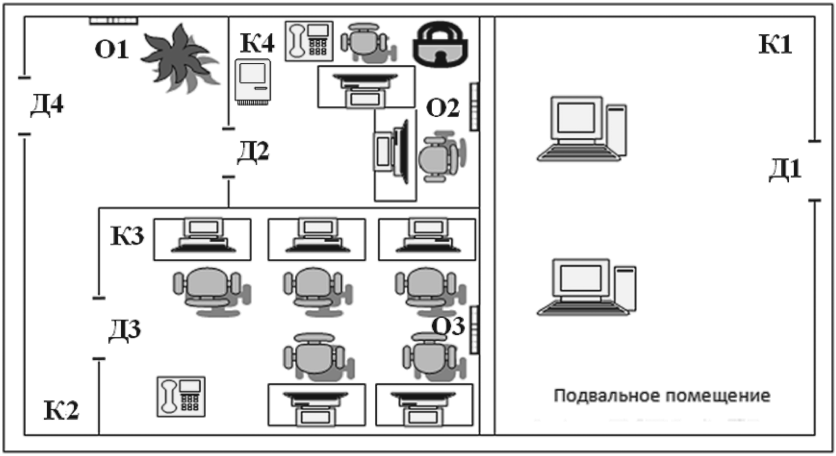


Рис. П3.2. Расположение помещений основного офиса компании

В комнате К3 постоянно находятся три системных администратора, секретарь и менеджер по продажам. Менеджер по обслуживанию продукции компании 1С и четвертый системный администратор практически все рабочее время находятся в разъездах по вызову клиента. Работа системных администраторов систематизирована дежурством «сутки — трое». Все ПО лицензированное.

Серверная комната располагается в помещении К1. Доступ в серверную комнату не регламентирован, как и в остальные комнаты. Ключи находятся в комнате К3 и доступны всем постоянным сотрудникам.

Данное подвальное помещение используется также как склад, на котором выполняются следующие основные операции:

- установка серверного оборудования для удаленного доступа к компьютерным приложениям клиентов;
- приемка техники по количеству и качеству;
- размещение техники и материалов;
- хранение;
- подготовка техники к отпуску в эксплуатации.

Коридор К2 находится под системой защиты предприятия, так как стены со стороны коридора стеклянные и имеется возможность подслушать разговор внутри комнат К3, К4.

Также в офисах К3 и К4 установлены стационарные телефоны для связи с клиентами и поставщиками.

Окна кабинетов оборудованы жалюзи и железными решетками. В серверной комнате окна отсутствуют, поскольку она находится в подвальном помещении. Все комнаты организации оборудованы системой пожарной сигнализации. Видеонаблюдение в офисе не ведется. Система охранной сигнализации отсутствует, поскольку в дневное время в офисе находятся сотрудники, а в ночное время и в выходные здание патрулируется охраной. Филиалы и представительства, а также дочерние предприятия отсутствуют.

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ..... 3

1. ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ МОДЕЛИ С ПОЛНЫМ ПЕРЕКРЫТИЕМ МНОЖЕСТВА УГРОЗ..... 5

1.1. Описание модели безопасности с полным перекрытием множества угроз 5

1.2. Порядок работы с программным инструментарием 7

1.3. Задания для моделирования СЗИ и требования к отчету 12

Контрольные вопросы и задания 13

2. АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ МЕТОДИКИ COBIT 14

2.1. Описание методики COBIT для анализа рисков информационной безопасности..... 14

2.2. Порядок работы с программным инструментарием Coras для анализа рисков информационной безопасности 22

2.3. Задания для анализа рисков информационной безопасности с использованием программного пакета Coras..... 30

Контрольные вопросы и задания 30

3. СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ ПАРЕТО-ОПТИМАЛЬНЫХ РЕШЕНИЙ В ОБЛАСТИ ПРОЕКТИРОВАНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ..... 32

3.1. Описание метода принятия решений в разработке системы защиты информации на основе закона Парето и метода достижимых целей 32

3.2. Порядок работы с программным инструментарием поддержки принятия парето-оптимальных решений 48

3.3. Задания для принятия решений по оценке альтернативных проектов защиты информации на основе закона Парето и метода достижимых целей 61

Контрольные вопросы и задания 62

4. АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОГО КОМПЛЕКСА ГРИФ 63

4.1. Описание программного комплекса ГРИФ для анализа и управления рисками информационных систем компаний 63

4.2. Пример анализа рисков информационной безопасности в системе дистанционного банковского обслуживания «Банк-Клиент» с использованием комплекса ГРИФ 66

4.3. Задания для анализа и управления рисками компании с использованием комплекса ГРИФ 73

Контрольные вопросы и задания 74

5. РАЗРАБОТКА СЦЕНАРИЕВ ДЕЙСТВИЙ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ СЕТИ ПЕТРИ 75

5.1. Особенности моделирования на основе сети Петри 75

5.2. Порядок работы с программным модулем VisualPetri 77

5.3. Задание для построения сценария действий нарушителя на объекте информатизации с использованием сети Петри 81

Контрольные вопросы и задания 82

6. ОПРЕДЕЛЕНИЕ ПОКАЗАТЕЛЕЙ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ПРИ НЕСАНКЦИОНИРОВАННОМ ДОСТУПЕ 83

6.1. Методы расчета прочности оболочки защиты 83

6.2. Задания для определения прочности оболочек защиты 87

Контрольные вопросы 88

СПИСОК ЛИТЕРАТУРЫ 89

ПРИЛОЖЕНИЕ 1

Варианты заданий 90

ПРИЛОЖЕНИЕ 2

Пример выполнения работы по анализу рисков информационной безопасности с использованием программы CORAS 104

ПРИЛОЖЕНИЕ 3

Общие сведения о компании 113

По вопросам приобретения книг обращайтесь:
Отдел продаж «ИНФРА-М» (оптовая продажа):
127282, Москва, ул. Полярная, д. 31В, стр. 1
Тел. (495) 380-4260; факс (495) 363-9212
E-mail: books@infra-m.ru

•

Отдел «Книга—почтой»:
тел. (495) 363-4260 (доб. 232, 246)

Учебное издание

Баранова Елена Константиновна
Бабаш Александр Владимирович

МОДЕЛИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

ПРАКТИКУМ

Учебное пособие

Подписано в печать 06.07.2014.
Формат 60×88/16. Гарнитура Newton.
Бумага офсетная. Печать офсетная.
Усл. печ. л. 7,35. Уч.-изд. л. 7,51.
Тираж 200 экз. Заказ №
Цена свободная.

ТК 475750-13365-060714

ООО «Издательский Центр РИОР»
127282, Москва, ул. Полярная, д. 31В.
info@rior.ru www.rior.ru

ООО «Научно-издательский центр ИНФРА-М»
127282, Москва, ул. Полярная, д. 31В, стр. 1.
Тел.: (495) 380-05-40, 380-05-43.
Факс: (495) 363-92-12
E-mail: books@infra-m.ru http://www.infra-m.ru