ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Практикум по курсу «Моделирование информационно-аналитических систем» является руководством для подготовки и проведения практических занятий в рамках изучения дисциплины «Моделирование информационно-аналитических систем» для студентов, обучающихся по специальности 10.05.04 «Информационно-аналитические системы безопасности».

В итоге освоения дисциплины на основе использования данного практикума обучающиеся приобретут навыки по разработке и применению математических моделей и методов анализа массивов данных и интерпретирования профессионального смысла получаемых формальных результатов; по использованию методов оценивания эффективности информационно-аналитических систем методами моделирования и разработке, обоснованию и реализации процедур решения задач профессиональной деятельности на основании совокупности существующих математических методов.

В практикуме представлено 16 практических занятий. В структуре практикума по каждому занятию представлены: тема занятия; время выполнения; методические указания к выполнению; ход выполнения работы; контрольные вопросы; источники.

В пункте «методические указания к выполнению» обозначены условия реализации и материально-технические требования к выполнению работы.

Пункт «Ход выполнения работы» содержит перечень заданий и алгоритм их выполнения. По ходу этапов алгоритма выполнения заданий, в том числе, представлены пояснения для реализации заданий. Первым этапом к выполнению всех работ является требование ответить на контрольные вопросы занятия. При выполнении ответов на контрольные вопросы студент к каждому ответу указывает ссылку на источник полученного ответа в соответствии с ГОСТ Р 7.0.100-2018 «Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Библиографическое описание. Общие требования и правила составления».

В пункте «Контрольные вопросы» обозначен перечень вопросов для самостоятельной работы студента. При защите выполненных заданий практического занятия контроль по данному пункту преподаватель выполняет в выбранной им форме. Варианты: письменный опрос; устный опрос; выполнение теста.

Требуемые (обязательные) источники для выполнения заданий представлены к каждому практическом занятию.

Практикум содержит 2 приложения. Приложение А содержит примеры представления данных по обработке и анализу результатов работы экспертной группы. Приложение используется на практических занятиях №12 и №13.

В приложении Б приведены примеры тестовых заданий для подготовки к практическому занятию №16.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 1-2
ИНФРАСТРУКТУРНОЕ МОДЕЛИРОВАНИЕ. ПОСТРОЕНИЕ АРХИТЕКТУРЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРЕДПРИЯТИЯ

Время выполнения: 4 часа.

Методические указания

Работа выполняется под руководством преподавателя. Обучаемые работают за ПЭВМ, имеющими доступ к сети Интернет.

Ход выполнения работы

1. Ответить на контрольные вопросы.

2. Для выполнения работы выбирается либо действующая организация (предприятие), либо проектируемая. Специфика работы организации выбирается самостоятельно. Организационно-содержательная составляющая по объекту работы может носить авторский характер исполнителя (достоверность исходных данных для работы не проверяется).

Ограничение на количество сотрудников организации (предприятия): должно быть не менее 15 и не более 100 человек.

Для выбранной организации (предприятия) необходимо:

2.1. Описать:

– наименование предприятия;

– организационно-правовую форму;

– сферу деятельности, отраслью, функционал;

– вид данных, обрабатываемых на предприятии. Для удобства работы используем классификацию, представленную на рис. 1;

– количество сотрудников;

– вид информационной системы (класс, вид по топологии).

2.2. Разработать:

– топологическую схему информационной системы (ИС) организации (предприятия). Варианты базовых топологических схем ИС представлены на рис. 2;

– организационно-структурную схему работы организации (предприятия) с обозначением кол-ва человек в каждом структурном подразделении - представить рисунком. Пример – см. рис. 3;

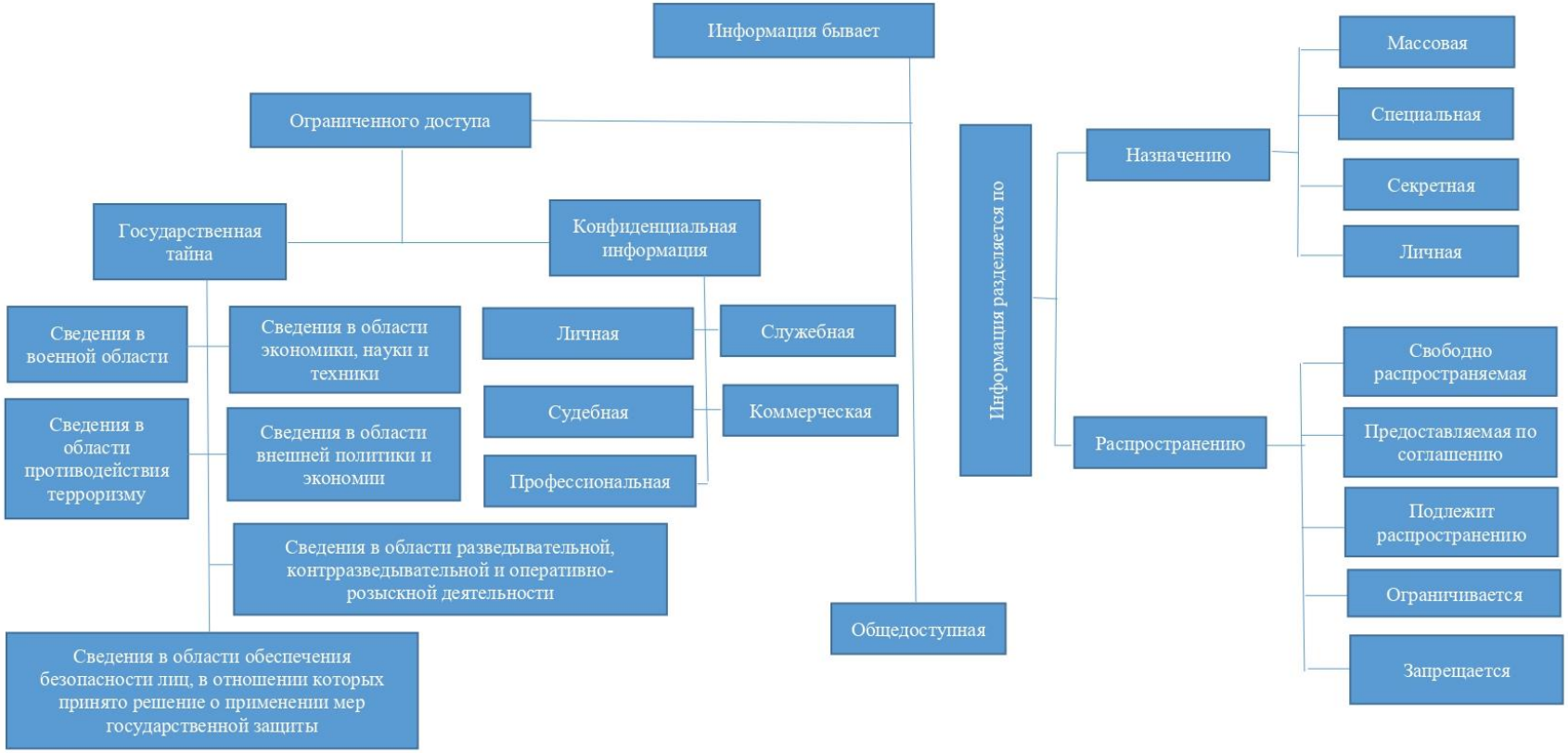
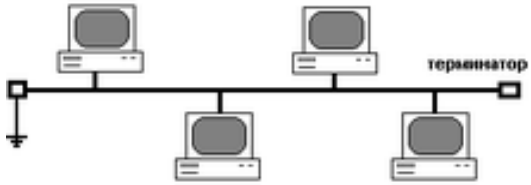
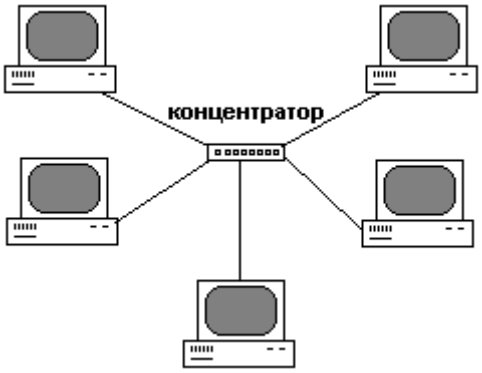


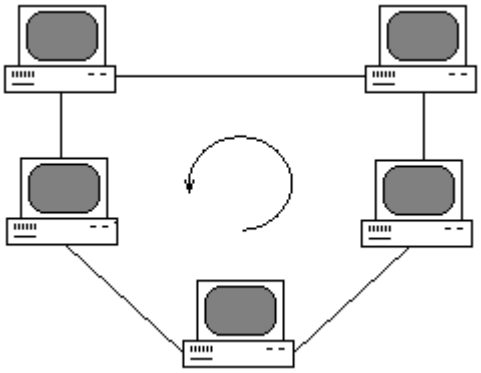
Рисунок 1. Классификация видов информации (https://habr.com/ru/company/vps_house/blog/343498/)



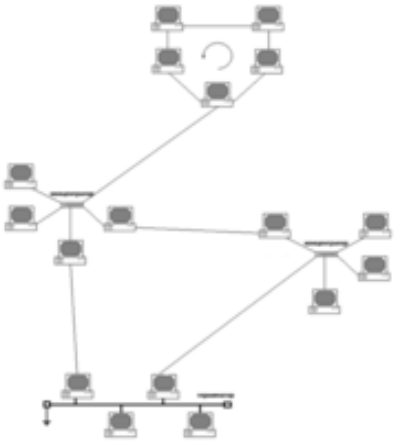
а) топология - шина



б) топология – звезда



в) топология – кольцо



г) комбинированная топология

Рисунок 2. Базовые варианты топологии систем и сетей

– проект визуализации точки зрения на архитектуру ИС. Пример – см. рис. 4.

3. Результаты выполненных заданий оформить в виде отчета по форме, установленной в РТУ МИРЭА.

Контрольные вопросы

1. Введите определения понятий: архитектура (системы), структура архитектуры, точка зрения на архитектуру, топология, информационная система, организация, предприятие, организационно-функциональная схема, защита информации, моделируемая система, мониторинг, информационной безопасности, аудит информационной безопасности.

2. Опишите алгоритм построения проекта архитектуры ИС организации (предприятия).

Рисунок 3. Пример организационно-структурной схемы работы организации (предприятия)

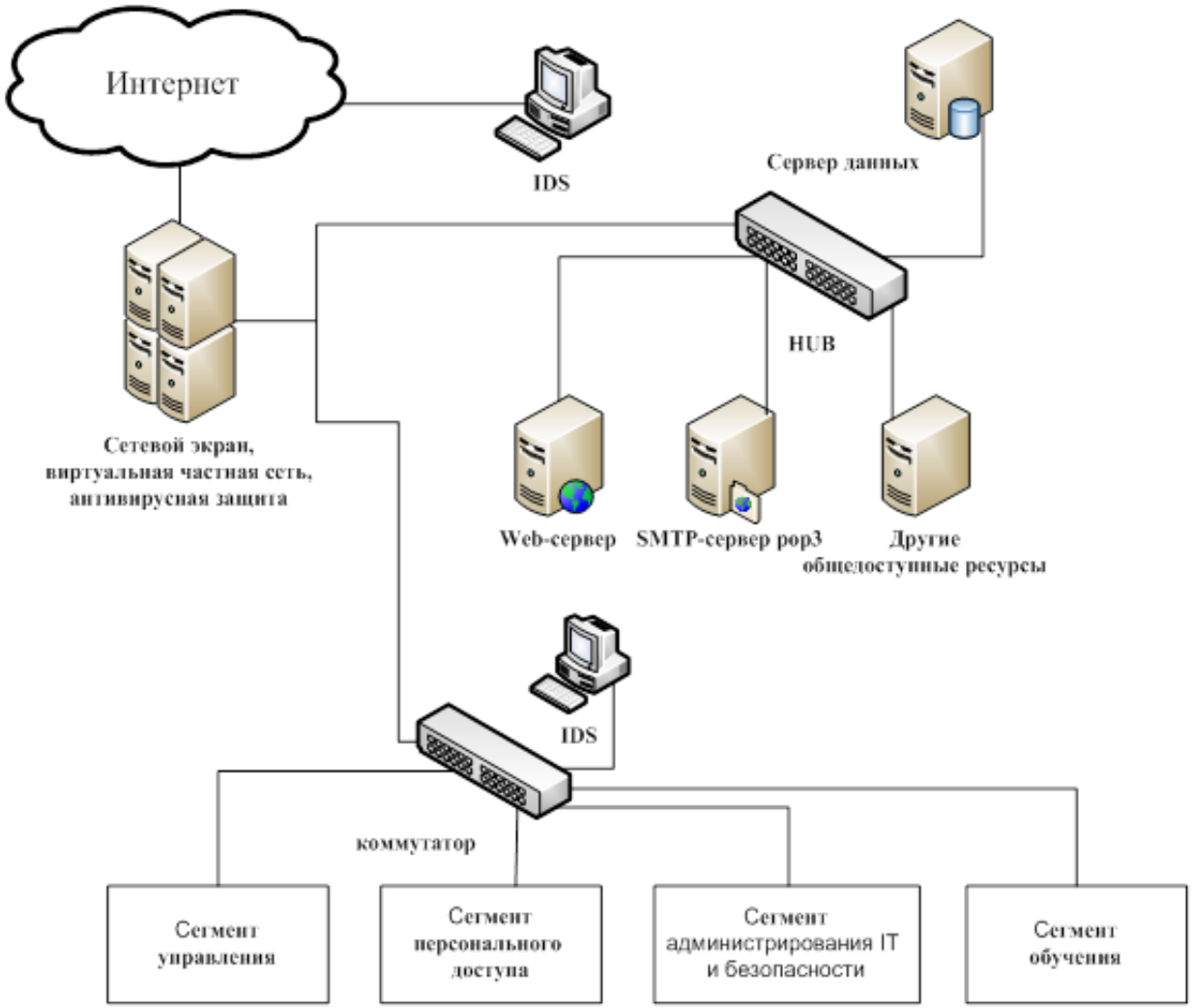


Рисунок 4. Пример визуализации точки зрения на архитектуру ИС для компании (подразделения компании), имеющей выход в Интернет и обладающей ресурсами, к которым необходим доступ из Интернета (https://konspekta.net/lek-6355.html)

Источники

1. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. – М.: Стандартинформ, 2018. – 8 с.

2. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. – М.: Стандартинформ, 2018. – 16 с.

3. ГОСТ Р 59347-2021 Системная инженерия. Защита информации в процессе определения архитектуры системы. – М.: Стандартинформ, 2021. – 38 с.

4. ГОСТ 58241 – 2018 Слаботочные системы. Кабельные системы. Магистральная подсистема структурированной кабельной системы. Основные положения. – М.: Стандартинформ, 2018. – 6 с.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 3
ПОСТРОЕНИЕ АРХИТЕКТУРЫ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ СИСТЕМЫ ПРЕДПРИЯТИЯ (ПРОДОЛЖЕНИЕ)

Время выполнения: 2 часа.

Методические указания

Работа выполняется под руководством преподавателя. Обучаемые работают за ПЭВМ, имеющих доступ в Интернет.

Ход выполнения работы

1. Ответить на контрольные вопросы.

2. Проанализировать виды информационно-аналитических систем (ИАС), использование которых возможно на предприятии. Работа выполняется по результатам выполнения практического занятия № 1-2.

Результат анализа представить в виде таблицы (форма представлена в табл. 1).

Таблица 1. Результаты анализа видов информационно-аналитических систем, использование которых возможно на предприятии «*название организации (предприятия), с которой(ым) выполняется работа*»

Вид ИАС	Описание ИАС (производитель, стоимость, преимущества, недостатки)	Решаемые задачи	Наименование элементов архитектуры ИС предприятия, используемых для работы ИАС	Ресурс, на котором установлена ИАС

3. Построить проект точки зрения на архитектуру ИАС для организации (предприятия) или ее подразделения.

4. Результаты выполненных заданий оформить в виде отчета по форме, установленной в РТУ МИРЭА.

Контрольные вопросы

1. Введите определение понятий: ИАС, функционал ИАС.
2. Представьте и опишите классификацию существующих ИАС.
3. Опишите наиболее распространенные ИАС.
4. Чем отличаются системы мониторинга ИБ, аудита ИБ от ИАС?

Источники

1. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. – М.: Стандартинформ, 2018. – 8 с.

2. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. – М.: Стандартинформ, 2018. – 16 с.

3. Белов В.С. Информационно-аналитические системы. Основы проектирования и применения: учебное пособие, руководство, практикум / Московский государственный университет экономики, статистики и информатики. — М., 2005. – 111 с.

4. Зариковская, Н.В. Информационно-аналитические системы управления: Учебное пособие [Электронный ресурс] / Н. В. Зариковская. — Томск: ТУСУР, 2018. – 107 с. – Режим доступа: https://edu.tusur.ru/publications/8233.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 4-5
РАЗРАБОТКА НЕФОРМАЛЬНОЙ МОДЕЛИ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ СИСТЕМЕ

Время выполнения: 4 часа.

Методические указания

Работа выполняется под руководством преподавателя. Обучаемые работают за ПЭВМ, имеющих доступ в Интернет.

Ход выполнения работы

Модель нарушителя ИБ строим для организации (предприятия), отработанной в практическом занятии № 1-2.

1. Ответить на контрольные вопросы.

2. Построить и описать стенд объекта защиты.

В качестве объекта защиты рассматривается ИАС, реализация которой возможна в организации (предприятии). Выбор осуществляется студентом самостоятельно, при согласовании с преподавателем. Для построения архитектуры ИАС определяется набор ее элементов и инфраструктура.

3. Согласно Банка данных угроз безопасности ФСТЭК России сформировать список не менее чем из 15 угроз ИБ для описанного в п. 2 объекта защиты. Список оформить в виде таблицы (форма – см. табл. 2).

Таблица 2. Список угроз ИБ объекта защиты (указать свой объект защиты)

№	Название угрозы ИБ	Описание угрозы ИБ	Код угрозы ИБ
1			
2			
….			

4. Руководствуясь Методикой оценки угроз безопасности информации ФСТЭК России разработать неформальную модель нарушителя ИБ описанного объекта защиты. В модели для каждой категории нарушителя заполнить соответствующие столбцы с показателями. К рассмотрению в модели принимается не менее 5 категорий нарушителя.

Пояснение. Показатели злоумышленника определяются в соответствии с методиками и документами из списка источников к данному практическому занятию.

5. Для представления неформальной модели нарушителя разработать и заполнить таблицу «Неформальная модель нарушителя ИБ ИАС организации (предприятия)……..».

6. Результаты выполненных заданий оформить в виде отчета по форме, установленной в РТУ МИРЭА.

Контрольные вопросы

1. Введите определения понятий: модель, злоумышленник, нарушитель, мотив, категория.

2. Опишите различные категории злоумышленников согласно документам регуляторов.

3. Опишите, как согласно методических указаний ФСТЭК России выполняется оценка возможностей нарушителя по реализации угроз безопасности информации.

4. Опишите, как согласно методических рекомендаций ФСБ России выполняется оценка возможностей нарушителя по реализации угроз безопасности информации.

5. Опишите структуру неформальной модели нарушителя ИБ.

Источники

1. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. – М.: Стандартинформ, 2018. – 8 с.

2. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. – М.: Стандартинформ, 2018. – 16 с.

3. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. – М.: Стандартинформ, 2018. – 8 с.

4. Методический документ. Методика оценки угроз безопасности информации (утв. ФСТЭК России 05 февраля 2021 г.).

5. Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных

данных, эксплуатируемых при осуществлении соответствующих видов деятельности (утв. ФСБ России 31 марта 2015 г. №149/7/2/6-432).

6. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»: Приказ ФСБ России от 10 июля 2014 г. № 378 (Зарегистрировано в Минюсте России 18 августа 2014 г. № 33620).

7. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (утв. ФСБ РФ 21 февраля 2008 г. N 149/54-144).

8. Банк данных угроз безопасности информации: ФСТЭК [Электронный ресурс]. – Режим доступа: https://bdu.fstec.ru.

9. Федеральная служба безопасности Российской Федерации [Электронный ресурс]. – Режим доступа: www.fsb.ru.

10. Федеральная служба по техническому и экспортному контролю России [Электронный ресурс]. – Режим доступа: https://fstec.ru.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 6-8
МОДЕЛИРОВАНИЕ ЗЛОУМЫШЛЕННЫХ ВОЗДЕЙСТВИЙ НА ИНФОРМАЦИОННО-АНАЛИТИЧЕСКУЮ СИСТЕМУ

Время выполнения: 4 часа.

Методические указания

Работа выполняется под руководством преподавателя. Обучаемые работают за ПЭВМ, имеющих доступ в Интернет. Ответы на контрольные вопросы выполняются студентом самостоятельно – внеаудиторно.

Ход выполнения работы

Модель нарушителя ИБ строим для организации (предприятия), отработанной в практическом занятии № 1-2.

1. Ответить на контрольные вопросы.

2. Разработать и исследовать формализованную D-модель злоумышленных воздействий на ИАС. По полученным результатам подготовить и оформить аналитический отчет.

2.1. Исходные данные

На систему воздействует 1 злоумышленник. Кол-во попыток несанкционированного доступа (НСД): 1, 2, 3, 4. Интенсивность воздействия:

$$\gamma = N \cdot 0{,}01,$$

где N - последние две цифры зачетки.

Задание по исходным данным 2.1

А.1. Разработать D-схему злоумышленных воздействий на ИАС для 1; 2; 3; 4 попыток НСД. В отчете представить полный вывод и решение полученных дифференциальных уравнений.

Пояснения. При создании D-схемы злоумышленных воздействий на ИАС принимаются следующие предположения:

1. Случайность во времени: каждая попытка НСД возникает с интервалом времени Δt, не зависящим от состояния системы и однозначно зависящим от некоторой константы (интенсивности нападений). Интенсивность во времени не меняется.

2. Отсутствие последействия: каждая последующая попытка НСД не зависит от предыдущих попыток. Это свойство присуще особой группе случайных процессов, называемых марковскими, поэтому часто называется марковостью.

3. Длительность самой попытки НСД намного меньше интервалов Δt между соседними попытками (гипотеза точечного воздействия).

При решении поставленной задачи рассматривается вероятность того, что за время *t* сделано *к* попыток НСД, равная $p_t(к)$. Обозначим интенсивность НСД через γ, считая, что за бесконечно малый интервал *dt* может произойти максимум одно событие, вероятность которого:

$$p(dt) = \gamma \cdot dt. \quad (1)$$

В данном случае возможно одно из двух событий:

Событие 1: за время *t* принято *К* попыток НСД, а за *dt* – ни одной. Вероятность такого сложного события:

$$p_1(к,t) = p_t(к) \cdot [1-\gamma \cdot dt]. \quad (2)$$

Событие 2: за время *t* произошло *к-1* попыток НСД, а за *dt* – одна; соответствующая вероятность:

$$p_2(к,t) = p_t(к-1) \cdot \gamma \cdot dt. \quad (3)$$

Вероятность группы описанных событий:

$$p(к,\ t+dt) = p_1(к,t) + p_2(к,t) = p_t(к) \cdot [1-\gamma \cdot dt] + p_t(к-1) \cdot \gamma \cdot dt. \quad (4)$$

Из (4) можно получить:

$$\frac{p(k,t+dt)-p(k,t)}{dt} = \gamma \cdot [p_t(k-1) - p_t(k)]. \quad (5)$$

Выражение слева в (5) можно обозначить через *dp(к,t)/dt*; тогда из (5) можно получать законы распределения для разных *к*.

Так, при *к = 0*, учитывая, что *p(-1) = 0*, получим:

$$\frac{p(0,t)}{dt} = -\gamma \cdot p_t(0).$$

Отсюда

$$\mathrm{p}(0,t) = e^{-\gamma \cdot t}. \quad (6)$$

Выражение (1.6) – это вероятность того, что за время t не произойдет ни одной попытки НСД. Как видим, распределение имеет чисто экспоненциальный характер. Отсюда следует, что вероятность того, что за время t произойдет хотя бы одна попытка НСД:

$$P_H = 1 - p(0,t) = 1 - e^{-\gamma t}. \quad (7)$$

Продолжая приведенные рассуждения, запишем выражение для вероятности однократного нарушения:

$$\frac{\mathrm{dp}(1,\mathrm{t})}{\mathrm{dt}} = \gamma[\mathrm{p}(0,\mathrm{t}) - \mathrm{p}(1,\mathrm{t})]. \quad (8)$$

Из (8) получим:

$$\frac{\mathrm{dp}(1,\mathrm{t})}{\mathrm{dt}} + \gamma \mathrm{p}(1,\mathrm{t}) = \gamma \mathrm{p}(0,\mathrm{t}) = \gamma \mathrm{e}^{-\gamma \mathrm{t}}. \quad (9)$$

Решение дифференциального уравнения (9) дает:

$$p(1,t) = \gamma \cdot t \cdot e^{-\gamma t}. \quad (10)$$

Рассуждая аналогично, для произвольного целого к получим:

$$\mathrm{p}(\mathrm{k},\mathrm{t}) = \frac{(\gamma \mathrm{t})^{\kappa}}{\kappa!}\mathrm{e}^{-\gamma \mathrm{t}} = \frac{\lambda^{\kappa}}{\kappa!}\mathrm{e}^{-\lambda}. \quad (11)$$

А.2. Выполнить моделирование злоумышленных воздействий на ИАС для 1, 2, 3, 4 попыток НСД в течение месяца с периодичностью 2 суток (графики в Excel).

Пояснения. При выполнении задания работа выполняется с формализованными моделями, полученными для различного количества попыток НСД, путем моделирования ситуаций при различных значениях входных параметров. Пример визуализации полученного одного из результатов (для *k=1*) см. на рис. 5.

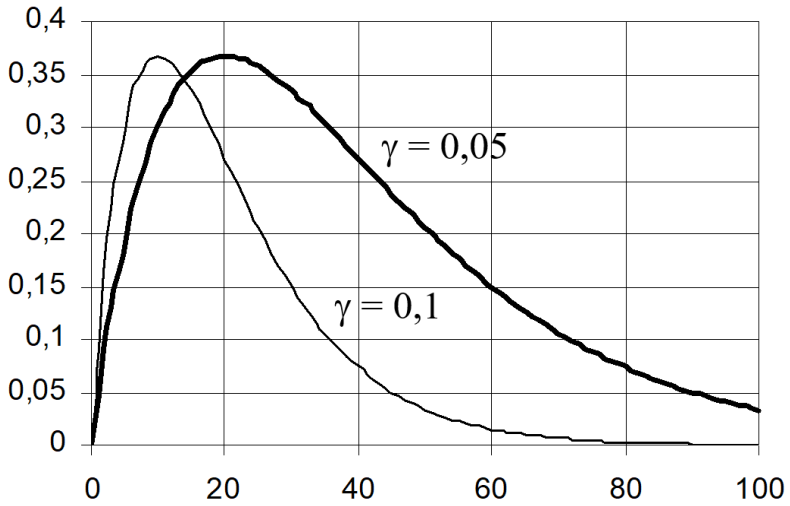


Рисунок 5. Визуализация результата моделирования злоумышленных воздействий для 1 попытки НСД (пример)

По каждому полученному результату должны быть сделаны выводы. Например, фрагмент выводов по рис. 5:

«В ходе моделирования злоумышленных воздействий на ИАС при 1 возможной попытки НСД получено следующее

1. При различных значениях γ вероятность однократной попытки НСД принимает максимальное значение 0,37.

2. Чем меньше γ тем быстрее наступает возможность реализации злоумышленных воздействий на систему.

3. При уменьшении значения γ время воздействия злоумышленника с наибольшим значением вероятности однократной попытки НСД увеличивается.

…….».

2.2. Исходные данные

На систему воздействует 2 злоумышленника. Кол-во попыток НСД: (1,1), (1, 2), (2,3). Интенсивность воздействия на ИАС первым злоумышленником равна N*0,01, Интенсивность воздействия на ИАС вторым злоумышленником γ=N·0,02, где N – последние две цифры зачетки.

Задание по исходным данным 2.2

Б.1. Разработать логическую модель несанкционированного доступа в ИАС двумя злоумышленниками;

Пояснения. При построении логической модели необходимо:

– сформулировать высказывание. На пример: «А - В процессе одновременного воздействия на систему двух злоумышленников НСД в систему будет получен, если подучен НСД хотя бы одним из злоумышленников»;

– декомпозировать сформулированное высказывание. Например: «А1 – первый злоумышленник получил НСД в систему, А2 - второй злоумышленник получил НСД в систему»;

– построить логическую модель. На пример:

$$A=(A1 \vee A2) /\backslash A1 /\backslash A2.$$

Б.2. Разработать D-схему злоумышленных воздействий на систему двумя злоумышленниками для 1, 2, 3, 4 попыток НСД в виде функции F-вероятность воздействия на систему двух злоумышленников;

Пояснения. При выполнении задания используем формализованные модели, полученные в А.1 и теоремы сумме и произведении вероятностей событий.

Б.3. Выполнить моделирование злоумышленных воздействий на систему в течении месяца с периодичностью 2 суток (графики в Excel).

Пояснения. При выполнении задания используем формализованную модель, полученные в Б.2 и пояснения к заданию А.2.

Б.4. Рассчитать ориентировочное значение количества попыток НСД нарушителем за 2 недели.

Пояснение. Ориентировочное значение количества попыток нарушителя за время $T_Н$ можно определить через математическое ожидание экспоненциального распределения (среднее значение $t_{н.ср}$):

$$t_{н.ср} = 1/\gamma.$$

Тогда:

$$N \cong \frac{T_Н}{t_{Н.СР}} = \gamma T_Н .$$

3. Результаты выполненных заданий оформить в виде отчета по форме, установленной в РТУ МИРЭА.

Контрольные вопросы

1. Введите определения понятий: формализованная модель, модель нарушителя ИБ, несанкционированный доступ, моделирование, логическая модель.

2. Опишите алгоритм построения формализованной D-модели нарушителя ИБ.

3. Опишите D-модель нарушителя ИБ при однократной попытке им получения НСД в ИАС.

4. Опишите D-модель нарушителя ИБ при двукратной попытке им получения НСД в ИАС.

5. Опишите D-модель нарушителя ИБ при n попытках им получения НСД в ИАС.

6. Как рассчитывается суммарная вероятность реализации n попыток НСД в систему, выполняемых двумя злоумышленниками?

7. Как рассчитывается ориентировочное значение количества попыток нарушителем НСД в систему за определенный временной период?

Источники

1. Соколов, А.В. Защита информации в распределенных корпоративных сетях и системах / Соколов А.В.// М.: ДМК Пресс. – 2002. – 656 с.

2. Курило, А.П. [и др.]. Обеспечение информационной безопасности бизнеса. – М.: БДЦ - пресс, 2005. – 512 с.

3. Харрис, Т. Теория ветвящихся случайных процессов / Харрис Т. // М: Мир. 1966 г. –355 с.

4. Прохоров, Ю.В. /Прохоров Ю.В., Розанов Ю.А.// Теория вероятностей. – М: Изд-во. Наука, 1973 г. – 395 с.

5. Горяйнов, В.В. О предельных распределениях вероятностей для докритических ветвящихся процессов / Горяйнов, В.В. Полковников А.А. // Теория вероятностей и ее применение. – Т.41. – вып.2. – 1996 г. – С. 417–424.

6. Максимова, Е.А. Цепи Маркова, как средство прогнозирования инсайдерских вторжений / Максимова Е.А., Корнева В.А., Витенбург Е.А. // Проблемы информационной безопасности. Компьютерные системы. – 2015. – № 4. – С. 9–12.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 9
РАЗРАБОТКА МОДЕЛИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ СИСТЕМЫ С ИСПОЛЬЗОВАНИЕМ КЛАССИФИКАТОРА

Время выполнения: 2 часа.

Методические указания

Работа выполняется под руководством преподавателя. Обучаемые работают за ПЭВМ, имеющих доступ в Интернет. Ответы на контрольные вопросы выполняются студентом самостоятельно – внеаудиторно.

Ход выполнения работы

1. Ответить на контрольные вопросы.

2. Ознакомиться с ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».

3.Определиться с объектом защиты (организацией (предприятием) или ИАС, отработанных в практических занятиях № 1–3).

4. Построить список угроз ИБ, реализация которых возможна на объекте защиты с использованием классификатора ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения». Количество угроз – 25.

5. Для полученного после выполнения пункта 4 списка угроз ИБ построить модель угроз ИБ в виде дерева угроз ИБ объекта защиты.

6. Модель угроз ИБ объекта защиты представить в логической форме.

7. Результаты выполненных заданий оформить в виде отчета по форме, установленной в РТУ МИРЭА.

Контрольные вопросы

1. Введите определения понятий: угроза, уязвимость, атака, инцидент, модель, модель угроз ИБ, дерево угроз ИБ.

2. Введите определения свойств информации: конфиденциальность, целостность, доступность.

3. Перечислите документы, являющиеся классификаторами угроз ИБ.

4. Опишите структуру классификатора угроз ИБ.

5. Опишите алгоритм построения модели угроз ИБ. Приведите пример.

6. Опишите алгоритм построения логической модели угроз ИБ. Приведите пример.

Источники

1. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. – М.: Стандартинформ, 2018. – 8 с.

2. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. – М.: Стандартинформ, 2018. – 16 с.

3. Банк данных угроз безопасности информации: ФСТЭК [Электронный ресурс]. – Режим доступа: https://bdu.fstec.ru.

4. Федеральная служба безопасности Российской Федерации [Электронный ресурс]. – Режим доступа: www.fsb.ru.

5. Федеральная служба по техническому и экспортному контролю России [Электронный ресурс]. – Режим доступа: https://fstec.ru.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 10-11
РАЗРАБОТКА МОДЕЛИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ СИСТЕМЫ ПО ТРЕБОВАНИЯМ ФСТЭК РОССИИ

Время выполнения: 2 часа.

Методические указания

Работа выполняется под руководством преподавателя. Обучаемые работают за ПЭВМ, имеющих доступ в Интернет. Ответы на контрольные вопросы выполняются студентом самостоятельно – внеаудиторно.

Ход выполнения работы

1. Ответить на контрольные вопросы.

2. Ознакомиться с банком данных угроз безопасности информации ФСТЭК России.

3. Определиться с объектом защиты (организацией (предприятием) или ИАС, отработанных в практических занятиях № 1-3).

4. Построить список угроз ИБ, реализация которых возможна на объекте защиты с использованием банка данных угроз безопасности информации ФСТЭК России. Количество угроз – 25.

5. Для полученного после выполнения пункта 4 списка угроз ИБ построить модель угроз ИБ в виде дерева угроз ИБ объекта защиты.

6. Модель угроз ИБ объекта защиты представить в логической форме.

7. Разработать контекстную диаграмму «Разработка модели угроз информационной безопасности» в нотации IDF0.

8. Результаты выполненных заданий оформить в виде отчета по форме, установленной в РТУ МИРЭА.

Контрольные вопросы

1. С указанием источника, введите определения следующих понятий: угроза, уязвимость, атака, деструктивное воздействие модель, модель угроз, дерево угроз, конфиденциальность, целостность, доступность информации.

2. Опишите, как согласно Методики оценки угроз безопасности информации, утв. ФСТЭК России 5 февраля 2021 г., выполняется построение модели угроз ИБ.

3. Опишите, как согласно Методики оценки угроз безопасности информации, утв. ФСТЭК России 5 февраля 2021 г., выполняется построение сценариев реализации угроз ИБ.

4. Опишите структуру банка данных угроз и уязвимостей ФСТЭК России.

5. Введите основные определения и правила построения контекстной диаграммы в нотации IDF0.

6. Опишите схему построения логической модели угроз ИБ. Приведите пример.

Источники

1. Методический документ. Методика оценки угроз безопасности информации (утв. ФСТЭК России 05 февраля 2021 г.).

2. Банк данных угроз безопасности информации: ФСТЭК [Электронный ресурс]. – Режим доступа: https://bdu.fstec.ru.

3. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных от 15 февраля 2008 г. [Электронный ресурс]. – Режим доступа: file:///C:/Users/Пользователь/Downloads/Базовая%20модель%20от%2015%20февраля%202008%20г.%20(1).pdf.

4. Федеральная служба безопасности Российской Федерации [Электронный ресурс]. – Режим доступа: www.fsb.ru.

5. Федеральная служба по техническому и экспортному контролю России [Электронный ресурс]. – Режим доступа: https://fstec.ru.

6. Р 50.1.028-2001. Информационные технологии поддержки жизненного цикла продукции. Методология функционального моделирования// Методология функционального моделирования IDEF0. – М.: Госстандарт России, 2018. – 54 с.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 12-13
РАЗРАБОТКА МОДЕЛИ АКТУАЛЬНЫХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Время выполнения: 4 часа.

Методические указания

Работа выполняется под руководством преподавателя. Обучаемые работают за ПЭВМ, имеющих доступ в Интернет. Ответы на контрольные вопросы выполняются студентом самостоятельно – внеаудиторно.

Ход выполнения работы

1. Ответить на контрольные вопросы.

2. Определиться с составом экспертной группы (не менее 3 экспертов) для определения модели актуальных угроз ИБ объекта защиты, по модели угроз ИБ, построенной в практических занятиях № 10-11 (далее – ЭГ).

3. Подготовить работу экспертной группы по определению актуальных угроз ИБ объекта защиты с использованием:

3.1. Метода непосредственной оценки.

3.2. Метода ранжирования.

3.3. Метода парных сравнений.

Рекомендации: для работы используется одна из моделей угроз ИБ, полученных в результате выполнения практических занятиях № 9-11. Список угроз ИБ для экспертной работы должен состоять не менее чем из 12 угроз (по каждому методу). Исходный набор угроз для экспертной работы одинаковый для всех методов. 12 угроз выбираются из ранее полученных моделей, содержащих не менее чем 25 угроз.

Для работы используем вспомогательные таблицы (см. табл. 3 и 4).

Таблица 3. Форма для работы эксперта «I» по методу непосредственной оценки и методу ранжирования

№ угрозы	Результаты мнения эксперта «I»
Угроза 1	
Угроза 2	

Угроза N	

Таблица 4. Форма для работы эксперта «I» по методу парных сравнений

Эксперт «I»	Угроза 1	Угроза 2	----------	Угроза N
Угроза 1	1			
Угроза 2		1		
----------			1	
Угроза N				1

4. Файлы с формами для работы экспертов представить в виде отдельного файла в формате pdf. В каждой из форм обозначить вопрос, на который эксперт должен отвечать. Например,

4.1. Для метода непосредственной оценки:

«Уважаемый эксперт, для работы Вам представлен набор угроз ИБ информационно-аналитической системы предприятия ООО «…..», функционирующего в сфере…….:

У1 – ….,

У2 – …..,

……

Просим Вас оценить возможность реализации каждой из обозначенных угроз ИБ на информационно-аналитическую систему предприятия и отразить свое мнение в таблице:

	У1	***У2***	***У3***	***------***	***Уm***
Оценка возможности реализации угрозы ИБ					

Шкала для оценивания: [0,1], где 0 – минимальная возможность реализации угрозы ИБ, 1 – максимальная возможность реализации угрозы ИБ».

4.2. Для метода парных сравнений:

«Уважаемый эксперт, для работы Вам представлен набор угроз ИБ информационно-аналитической системы предприятия ООО «…..», функционирующего в сфере……:

У1 – ….,

У2 – …..,

……

Просим Вас оценить возможность реализации обозначенных угроз ИБ на информационно-аналитическую систему предприятия при попарном их сравнении и отразить свое мнение в таблице:

Эксперт «m»	Угроза 1	Угроза 2	----------	Угроза N
Угроза 1	1			
Угроза 2		1		
----------		p_{ij}^{m}	1	
Угроза N				1

Шкала для оценивания:

$$p_{ij}^{m} = \begin{cases} 1, \text{если угроза } p_i \text{ равнозначна угрозе } p_j \\ 0, \text{если угроза } p_i \text{ менее значима, чем угроза } p_j \\ 2, \text{если угроза } p_i \text{ более значима чем угроза } p_j \end{cases}$$

5. Для каждого из методов (3.1-3.3) выполнить сбор экспертных данных.

Рекомендации:

По методу непосредственной оценки эксперт присваивает каждому объекту числовое значение, например, определяет вероятность реализации угрозы.

По методу ранжирования эксперт присваивает объектам ранги, в порядке предпочтений.

По методу парных сравнений эксперт попарно сравнивает значимость объектов.

6. Для каждого из методов (3.1-3.3) выполнить обработку экспертных данных.

Рекомендации: результаты работы экспертов и обработка результатов экспертного опроса выполнять в редакторе Excel.

Для обработки результатов использовать формулы:

– для метода непосредственной оценки:

$$P(i) = \sum_{j=1}^{M} \frac{1}{M} \cdot p_{ij},$$

– для метода ранжирования:

$$rang(i) = \sum_{j=1}^{M} rang_{ij},$$

– для метода парных сравнений:

$$P(i) = \sum_{J=1}^{N} \sum_{m=1}^{M} \frac{1}{M \cdot N} \cdot p_{ij}^{m}.$$

7. По результатам п. 6 выполнить анализ полученных результатов, выбрать по 6 наиболее актуальных угроз ИБ.

8. По результатам п. 7 для каждого из методов построить модели актуальных угроз ИБ. Представить их в виде дерева угроз ИБ.

9. Выполнить сравнительный анализ результатов реализации экспертных методов при построении модели актуальных угроз ИБ ИАС.

10. Результаты выполненных заданий оформить в виде отчета по форме, установленной в РТУ МИРЭА.

Рекомендации: примеры оформления оценки и анализа результатов экспертной оценки в отчете представлены в Приложении А.

Контрольные вопросы

1. Чем отличается модель угроз ИБ от модели актуальных угроз ИБ?

2. Опишите работу метода непосредственной оценки при построении модели актуальных угроз ИБ.

3. Опишите работу метода ранжирования при построении модели актуальных угроз ИБ.

4. Опишите работу метода парных сравнений при построении модели актуальных угроз ИБ.

5. Опишите методику и этапы работы с экспертной группой при построении модели актуальных угроз ИБ.

Источники

1. Методический документ. Методика оценки угроз безопасности информации (утв. ФСТЭК России 05 февраля 2021 г.).

2. Банк данных угроз безопасности информации: ФСТЭК [Электронный ресурс]. – Режим доступа: https://bdu.fstec.ru.

3. Р 50.1.028-2001. Информационные технологии поддержки жизненного цикла продукции. Методология функционального моделирования// Методология функционального моделирования IDEF0. – М.: Госстандарт России, 2018. – 54 с.

4. Федеральная служба безопасности Российской Федерации [Электронный ресурс]. – Режим доступа: www.fsb.ru.

5. Федеральная служба по техническому и экспортному контролю России [Электронный ресурс]. – Режим доступа: https://fstec.ru.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 14-15
НЕЧЕТКОЕ МОДЕЛИРОВАНИЕ СИТУАЦИЙ РАЗВИТИЯ СОБЫТИЙ В ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ СИСТЕМЕ

Время выполнения: 4 часа.

Методические указания

Работа выполняется под руководством преподавателя. Обучаемые работают за ПЭВМ, имеющих доступ в Интернет. Ответы на контрольные вопросы выполняются студентом самостоятельно – внеаудиторно.

Ход выполнения работы

1. Ответить на контрольные вопросы.

2. Ознакомиться с функционалом и методикой работы в СППР Mind Modeler и СППР «ИГЛА».

3. Сформулировать и описать целевую функцию (концепт) для моделирования ИАС. При описании целевой функции (концепта) в том числе привести определения ключевых слов (ее составляющих) со ссылкой на источники. Дальнейшее название модели определяется контекстом целевой функции.

Варианты целевых функций (концептов) для моделирования ИАС:

1) Fc – Оценка информационной безопасности ИАС.
2) Fc – Оценка эффективности средств защиты ИАС.
3) Fc – Оценка возможностей нарушителя ИБ ИАС.
4) Fc – Оценка актуальности угроз ИБ ИАС.
5) Fc – Оценка функциональности ИАС.
6) Fc – Оценка возможности нарушения ИБ в ИАС.
7) Fc – Оценка рисков ИБ ИАС.
8) Fc – Оценка инвестиционных рисков при модернизации системы защиты ИАС.
9) Fc – Оценка надежности ИАС.
10) Fc – Оценка целостности ИАС.
11) Fc – Оценка возможности получения НСД к работе с данными в ИАС.
12) Fc – Оценка рисков информационной безопасности.
13) Fc – Оценка возможности несанкционированного доступа в ИАС.
14) Fc – Оценка значимости информационных ресурсов.
15) Fc – Оценка точности используемого алгоритма.

16) Fc – Комплексная оценка ИБ объекта защиты.

18) Fc – Оценка уровня компетентности кадров.

19) Fc –Оценка конкурентоспособности бизнеса.

20) Fc – Оценка качества предоставляемых услуг по …..

21) Fc – Оценка качества системы управления ИБ.

22) Fc – Оценка степени соответствия обеспечения ИБ организации требованиям…… (*указать документ*)

23) Fc – Оценка ИБ на основе … (*указать документ*)

24) Fc – Оценка точности оценки рисков ИБ.

25) Fc – Оценка степени согласованности экспертов.

4. Определить и сформулировать факторы влияния на реализацию целевой функции (концепта). Количество факторов (F[i]) – не менее 6.

Пояснения. Всякое событие, произошедшее в системе, вызывается определенными причинами (предпосылками), появление которых связано с движением материальных потоков (например, ресурсы) и нематериальных потоков (например, информационные взаимодействия). Движение каждого потока может быть описано в самом общем виде соответствующими цепочками причинно-следственных отношений, составляющих знания аналитика или его предположения о действующих в данной системе закономерностях. Вычленение таких потоков является первым шагом при когнитивном анализе исследуемой системы; каждый из выделенных потоков описывается соответствующей совокупностью факторов. Объединение всех этих совокупностей составляет множество факторов, в терминах которых описываются процессы в системе.

5. Определить взаимосвязи между факторами и вес межфакторного влияния. Результаты межфакторных взаимосвязей представить в таблице. Форма таблицы – табл. 5. Значения связей в таблице указывать в пределах от «-1» до «+1».

Пояснения. Определение взаимосвязи между факторами выполняется путем рассмотрения причинно-следственных цепочек, описывающих движение каждого потока. Считается, что факторы, входящие в первую часть «если...» цепочки «если – то», влияют на факторы ее второй части «то...», причем это влияние может быть либо усиливающим (положительным), либо тормозящим (отрицательным), либо переменного знака в зависимости от возможных дополнительных условий. Например, если в таблице на пересечении F1 и F4 определено значение «+0.3», то это значит, что что при увеличении значения влияния фактора F1 происходит увеличение значимости фактора F4 на +0.3

единицы по шкале [0;+1]. Если в таблице на пересечении F1 и F4 определено значение «-0.3», то это значит, что что при увеличении значения влияния фактора F1 происходит уменьшение значимости фактора F4 на 0.3 единицы по шкале [-1;0].

Таблица 5. Таблица межфакторного взаимодействия в модели «…….»
(*указывается название модели, с которой выполняется работа*)

	Fc	F[1]	F[2]	F[3]	F[4]	F[5]	F[6]
Fc	0						
F[1]		0					
F[2]			0				
F[3]				0			
F[4]					0		
F[5]						0	
F[6]							0

6. Используя программу MentalModeler построить когнитивную карту модели. Пример вариантов визуализации когнитивной карты нечеткой модели представлен на рис. 6-7.

Пояснения. Элементы в когнитивной карте могут быть обозначены либо прописаны через их наименования (рис. 6), либо через присвоенные им коды (рис. 7).

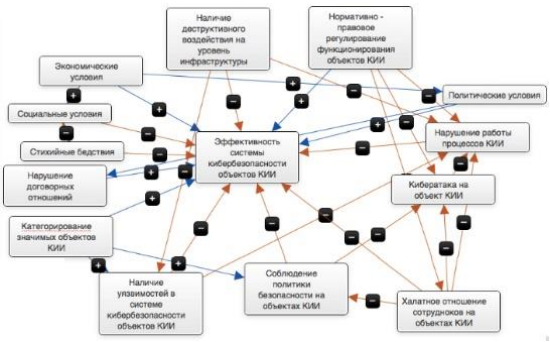


Рисунок 6. Визуализация примера когнитивной карты модели оценки эффективности системы обеспечения кибербезопасности объектов КИИ

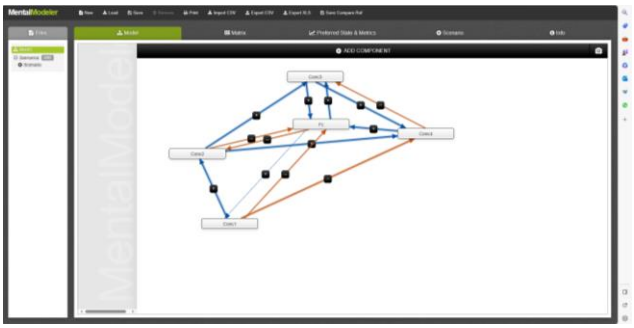


Рисунок 7. Пример когнитивной карты нечеткой модели, выполненной в среде MentalModeler

При построении когнитивной карты блоки, в которых размещены ее элементы, смещаем в плоскости построения с целью получения наилучшей визуализации модели.

Значения межфакторных связей проставляем либо в плоскости построения когнитивной карты (во вкладке «Model»), либо при заполнении матрицы во вкладке «Matrix». Пример построенной матрицы межфакторного влияния в нечеткой модели представлен на рис. 8.

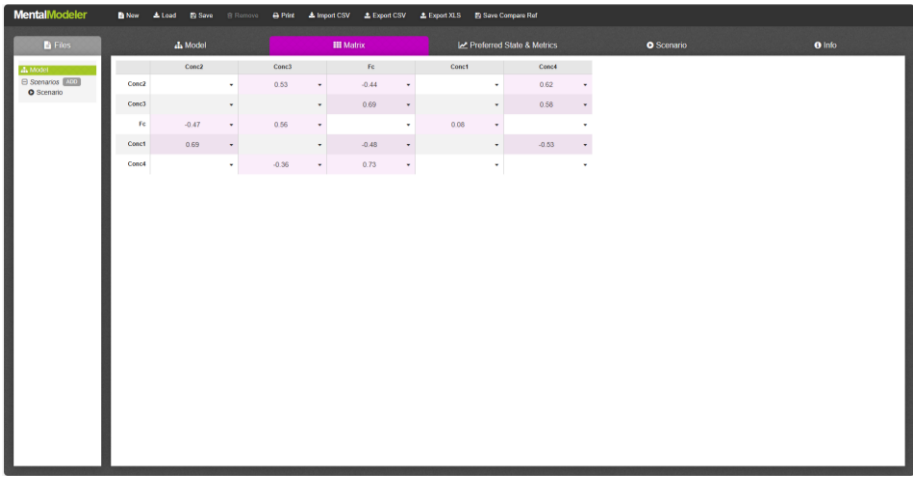


Рисунок 8. Пример матрицы межфакторного влияния в нечеткой модели, выполненной в системе MentalModeler

7. По выполненной нечеткой модели провести статический анализ.

Пояснения. Для выполнения задания анализируются данные оценочной матрицы с вкладки Preferred State & Metrics (Пример – см. рис. 9). В отчете необходимо описать значения по каждому из качественных показателей матрицы.

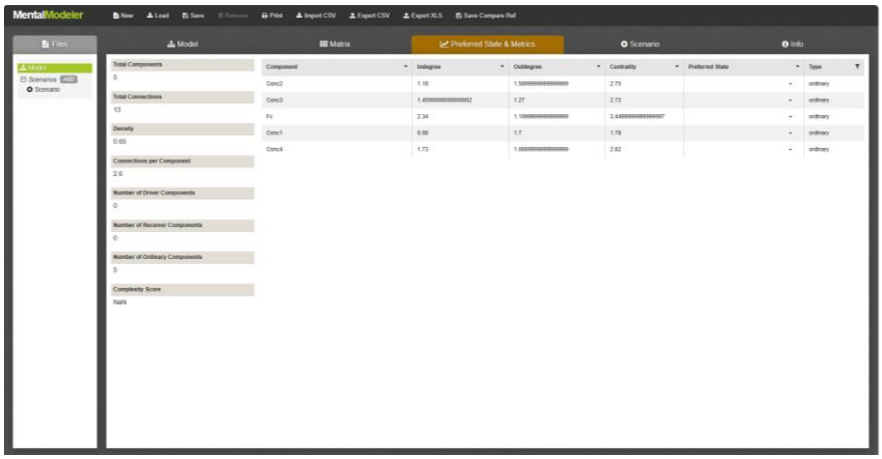


Рисунок 9. Пример данных оценочной матрицы с вкладки Preferred State & Metrics, реализованной в системе MentalModeler, для выполнения статического анализа нечеткой модели

8. Разработать план проведения экспериментального исследования нечеткой модели. Продумать и описать возможные сценарии развития событий. Прописать по каждому сценарию возможные альтернативы.

Форма для представления плана проведения экспериментального исследования нечеткой модели – см. табл. 6.

Таблица 6. Форма для представления плана проведения экспериментального исследования нечеткой модели

№ эксперимента	Цель	Изменяемый фактор (концепт)	Диапазон изменения	Шаг изменения	Наблюдаемые факторы (концепты)	Предполагаемый результат

Пояснения. При планировании экспериментального исследования необходимо рассмотреть сценарии, в которых будут изменяться:

1) только один концепт);

2) два фактора (концепта);

3) три фактора (концепта).

Выбор изменяемых концептов выбирается самостоятельно.

В сценариях 2 и 3 рассмотреть серию экспериментов, в которых необходимо предусмотреть различные варианты одновременного изменения их значений.

9. Провести экспериментальное исследование нечеткой модели согласно разработанного плана.

Пояснение. Если в ходе моделирования не проявляется динамика модели, то рекомендуется:

1) план проведения эксперимента дополнить, путем введения новых концептов, в качестве изменяемых. Отсутствие динамики (импульсного влияния) в модели говорит о том, что выбранные концепты оказывают незначительное влияние на модель;

2) изменить значения межфакторного влияния, относительно изменяемых концептов.

10. Описать ход выполнения каждого эксперимента с представлением сканов соответствующих интерфейсов с комментариями и пояснениями.

11. Выполнить пп. 6 – 10 в СППР «ИГЛА» (для самостоятельной работы).

Пояснение. Примеры экранных копий интерфейсов при выполнении заданий в СППР «ИГЛА» представлены на рис. 10.

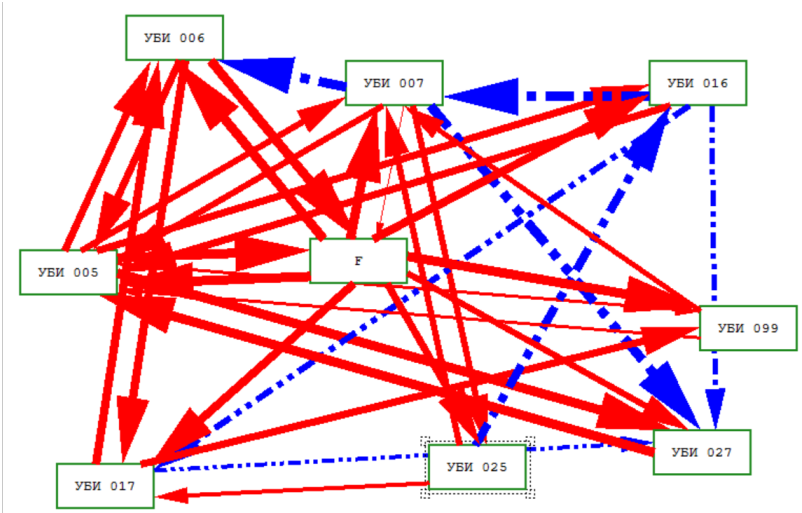
12. Результаты выполненных заданий оформить в виде отчета по форме, установленной в РТУ МИРЭА.

№	Название коцепта	Тип концепта	Целевой	Группа	Описание концепта
1	УБИ 005	Неуправл...	☐		
2	УБИ 006	Неуправл...	☐		
3	УБИ 007	Неуправл...	☐		
4	УБИ 016	Неуправл...	☐		
5	УБИ 017	Неуправл...	☐		
6	УБИ 025	Неуправл...	☐		
7	УБИ 027	Неуправл...	☐		
8	УБИ 099	Неуправл...	☐		
9	F	Управля...	☑		

10.1. Экранная копия интерфейса с видами концептов когнитивной модели

	УБИ 005	УБИ 006	УБИ 007	УБИ 016	УБИ 017	УБИ 025	УБИ 027	УБИ 099	F
УБИ 005	0	0,75	0,6	0,7	0	0	0,9	0,3	0,9
УБИ 006	0,75	0	0,16	0	0,89	0,12	0	0	0,92
УБИ 007	0,6	-0,92	0	0	0	0,62	-0,98	0,27	0,18
▸ УБИ 016	0,7	0	-0,95	0	-0,68	0	-0,56	0	0,84
УБИ 017	0	0,89	0	0	0	0	-0,45	0,73	0,71
УБИ 025	0	0	0,62	-0,82	0,4	0	0	0	0,39
УБИ 027	0,9	0,3	0	0	0	0	0,17	0	0,33
УБИ 099	0,3	0	0,56	0	0	0	0	0	0,6
F	0,9	0,15	0,93	0,6	0,29	0,79	0,66	0,99	0

10.2. Экранная копия интерфейса с нечеткой когнитивной матрицей



10.3. Экранная копия интерфейса с визуальным отображением когнитивной карты

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
▸ 1	0,8100	0,7382	0,8280	0,7700	0,8370	0,7268	0,7650	0,6022	0,7369	0,6853	0,7110	0,5597	0,9000	0,8203	0,8910	0,7014	0,9000	0,7084
2	0,7382	0,8100	0,7700	0,8280	0,7268	0,8370	0,6022	0,7650	0,6853	0,7369	0,5597	0,7110	0,8203	0,9000	0,7014	0,8910	0,7084	0,9000
3	0,8280	0,7546	0,8464	0,7872	0,8556	0,7429	0,7820	0,6156	0,8900	0,7006	0,7268	0,5721	0,7452	0,8385	0,9108	0,7169	0,9200	0,7242
4	0,7546	0,8280	0,7872	0,8464	0,7429	0,8556	0,6156	0,7820	0,7006	0,8900	0,5721	0,7268	0,8385	0,7452	0,7169	0,9108	0,7242	0,9200
5	0,6943	0,8820	0,7242	0,9200	0,6835	0,7872	0,5663	0,7194	0,6445	0,8188	0,6200	0,6687	0,7714	0,9800	0,6596	0,8379	0,6662	0,8464
6	0,8820	0,6943	0,9200	0,7242	0,7872	0,6835	0,7194	0,5663	0,8188	0,6445	0,6687	0,6200	0,9800	0,7714	0,8379	0,6596	0,8464	0,6662
7	0,8379	0,6596	0,8740	0,6880	0,7478	0,9500	0,6835	0,5380	0,7779	0,6800	0,6352	0,5890	0,9310	0,7328	0,7960	0,6266	0,8041	0,6329
8	0,6596	0,8379	0,6880	0,8740	0,9500	0,7478	0,5380	0,6835	0,6800	0,7779	0,5890	0,6352	0,7328	0,9310	0,6266	0,7960	0,6329	0,8041
9	0,7369	0,6716	0,8900	0,7006	0,7615	0,6612	0,6960	0,5478	0,7921	0,6235	0,6469	0,5092	0,6632	0,7463	0,8106	0,6381	0,8188	0,6445
10	0,6716	0,7369	0,7006	0,8900	0,6612	0,7615	0,5478	0,6960	0,6235	0,7921	0,5092	0,6469	0,7463	0,6632	0,6381	0,8106	0,6445	0,8188
11	0,5408	0,6871	0,5641	0,7167	0,7790	0,6132	0,4412	0,8200	0,5576	0,6378	0,4830	0,5209	0,6009	0,7634	0,5138	0,6528	0,5190	0,6593
12	0,6871	0,5408	0,7167	0,5641	0,6132	0,7790	0,8200	0,4412	0,6378	0,5576	0,5209	0,4830	0,7634	0,6009	0,6528	0,5138	0,6593	0,5190
13	0,9000	0,6644	0,7452	0,6930	0,7533	0,6541	0,6885	0,5420	0,6632	0,6168	0,6399	0,5037	0,8100	0,7382	0,8019	0,6312	0,8100	0,6376
14	0,6644	0,9000	0,6930	0,7452	0,6541	0,7533	0,5420	0,6885	0,6168	0,6632	0,5037	0,6399	0,7382	0,8100	0,6312	0,8019	0,6376	0,8100
15	0,3888	0,4939	0,4055	0,5152	0,5600	0,4408	0,3171	0,4029	0,3609	0,4585	0,3472	0,3744	0,4320	0,5488	0,3694	0,4692	0,3731	0,4740
16	0,4939	0,3888	0,5152	0,4055	0,4408	0,5600	0,4029	0,3171	0,4585	0,3609	0,3744	0,3472	0,5488	0,4320	0,4692	0,3694	0,4740	0,3731
17	0,9000	0,8203	0,9200	0,8556	0,9300	0,8075	0,8500	0,6691	0,8188	0,7615	0,7900	0,6219	0,8100	0,9114	0,9900	0,7793	0,8464	0,7872
18	0,8203	0,9000	0,8556	0,9200	0,8075	0,9300	0,6691	0,8500	0,7615	0,8188	0,6219	0,7900	0,9114	0,8100	0,7793	0,9900	0,7872	0,8464

10.4. Экранная копия интерфейса по результатам статического моделирования: Транзитивно замкнутая матрица

	1	2	3	4	5	6	7	8	9
1	0,8100	0,8280	0,8370	0,7650	0,7369	0,7110	0,9000	0,8910	0,9000
2	0,8280	0,8464	0,8556	0,7820	0,8900	0,7268	0,7452	0,9108	0,9200
3	0,6943	0,7242	0,6835	0,5663	0,6445	0,6200	0,7714	0,6596	0,6662
4	0,8379	0,8740	0,7478	0,6835	0,7779	0,6352	0,9310	0,7960	0,8041
5	0,7369	0,8900	0,7615	0,6960	0,7921	0,6469	0,6632	0,8106	0,8188
6	0,5408	0,5641	0,7790	0,4412	0,5576	0,4830	0,6009	0,5138	0,5190
7	0,9000	0,7452	0,7533	0,6885	0,6632	0,6399	0,8100	0,8019	0,8100
8	0,3888	0,4055	0,5600	0,3171	0,3609	0,3472	0,4320	0,3694	0,3731
9	0,9000	0,9200	0,9300	0,8500	0,8188	0,7900	0,8100	0,9900	0,8464

10.5. Экранная копия интерфейса по результатам статического моделирования: Положительно транзитивно замкнутая матрица

	1	2	3	4	5	6	7	8	9
1	-0,7382	-0,7700	-0,7268	-0,6022	-0,6853	-0,5597	-0,8203	-0,7014	-0,7084
2	-0,7546	-0,7872	-0,7429	-0,6156	-0,7006	-0,5721	-0,8385	-0,7169	-0,7242
3	-0,8820	-0,9200	-0,7872	-0,7194	-0,8188	-0,6687	-0,9800	-0,8379	-0,8464
4	-0,6596	-0,6880	-0,9500	-0,5380	-0,6800	-0,5890	-0,7328	-0,6266	-0,6329
5	-0,6716	-0,7006	-0,6612	-0,5478	-0,6235	-0,5092	-0,7463	-0,6381	-0,6445
6	-0,6871	-0,7167	-0,6132	-0,8200	-0,6378	-0,5209	-0,7634	-0,6528	-0,6593
7	-0,6644	-0,6930	-0,6541	-0,5420	-0,6168	-0,5037	-0,7382	-0,6312	-0,6376
8	-0,4939	-0,5152	-0,4408	-0,4029	-0,4585	-0,3744	-0,5488	-0,4692	-0,4740
9	-0,8203	-0,8556	-0,8075	-0,6691	-0,7615	-0,6219	-0,9114	-0,7793	-0,7872

10.6. Экранная копия интерфейса по результатам статического моделирования: Отрицательно транзитивно замкнутая матрица

	1	2	3	4	5	6	7	8	9
1	0,8100	0,8280	0,8370	0,7650	0,7369	0,7110	0,9000	0,8910	0,9000
2	0,8280	0,8464	0,8556	0,7820	0,8900	0,7268	-0,8385	0,9108	0,9200
3	-0,8820	-0,9200	-0,7872	-0,7194	-0,8188	-0,6687	-0,9800	-0,8379	-0,8464
4	0,8379	0,8740	-0,9500	0,6835	0,7779	0,6352	0,9310	0,7960	0,8041
5	0,7369	0,8900	0,7615	0,6960	0,7921	0,6469	-0,7463	0,8106	0,8188
6	-0,6871	-0,7167	0,7790	-0,8200	-0,6378	-0,5209	-0,7634	-0,6528	-0,6593
7	0,9000	0,7452	0,7533	0,6885	0,6632	0,6399	0,8100	0,8019	0,8100
8	-0,4939	-0,5152	0,5600	-0,4029	-0,4585	-0,3744	-0,5488	-0,4692	-0,4740
9	0,9000	0,9200	0,9300	0,8500	0,8188	0,7900	-0,9114	0,9900	0,8464

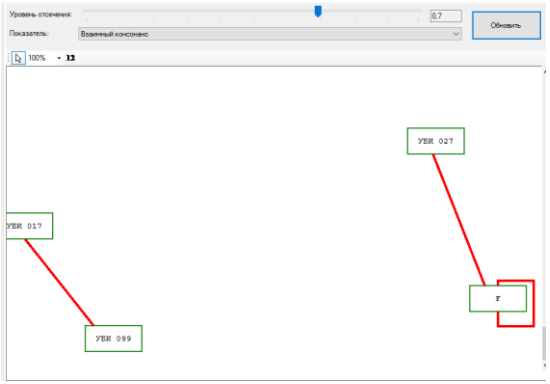
10.7. Экранная копия интерфейса по результатам статического моделирования: Матрица влияния

	1	2	3	4	5	6	7	8	9
1	0,0464	0,0363	0,0705	0,1191	0,0363	0,1191	0,0464	0,1191	0,1191
2	0,0464	0,0363	0,0705	0,1191	0,1191	0,1191	0,0589	0,1191	0,1191
3	0,1191	0,1191	0,0705	0,1191	0,1191	0,0378	0,1191	0,1191	0,1191
4	0,1191	0,1191	0,1191	0,1191	0,0671	0,0378	0,1191	0,1191	0,1191
5	0,0464	0,1191	0,0705	0,1191	0,1191	0,1191	0,0589	0,1191	0,1191
6	0,1191	0,1191	0,1191	0,3004	0,0671	0,0378	0,1191	0,1191	0,1191
7	0,1506	0,0363	0,0705	0,1191	0,0363	0,1191	0,0464	0,1191	0,1191
8	0,1191	0,1191	0,1191	0,1191	0,1191	0,0378	0,1191	0,1191	0,1191
9	0,0464	0,0363	0,0705	0,1191	0,0363	0,1191	0,0589	0,1191	0,0363

10.8. Экранная копия интерфейса по результатам статического моделирования: Матрица консонанса влияния

	1	2	3	4	5	6	7	8	9
1	0,9536	0,9637	0,9295	0,8809	0,9637	0,8809	0,9536	0,8809	0,8809
2	0,9536	0,9637	0,9295	0,8809	0,8809	0,8809	0,9411	0,8809	0,8809
3	0,8809	0,8809	0,9295	0,8809	0,8809	0,9622	0,8809	0,8809	0,8809
4	0,8809	0,8809	0,8809	0,8809	0,9329	0,9622	0,8809	0,8809	0,8809
5	0,9536	0,8809	0,9295	0,8809	0,8809	0,8809	0,9411	0,8809	0,8809
6	0,8809	0,8809	0,8809	0,6996	0,9329	0,9622	0,8809	0,8809	0,8809
7	0,8494	0,9637	0,9295	0,8809	0,9637	0,8809	0,9536	0,8809	0,8809
8	0,8809	0,8809	0,8809	0,8809	0,8809	0,9622	0,8809	0,8809	0,8809
9	0,9536	0,9637	0,9295	0,8809	0,9637	0,8809	0,9411	0,8809	0,9637

10.9. Экранная копия интерфейса по результатам статического моделирования: Матрица диссонанса влияния



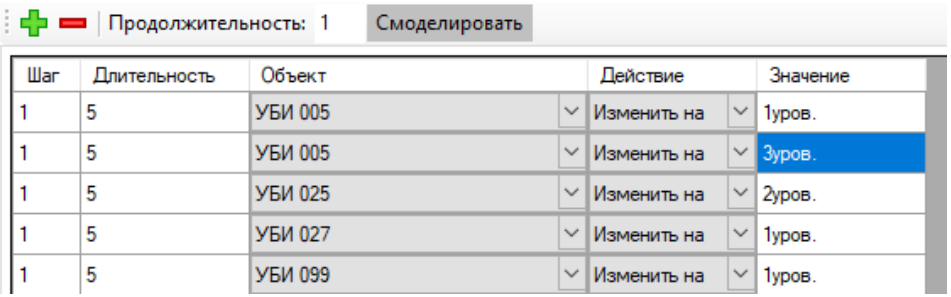
10.10. Экранная копия интерфейса по результатам статического моделирования: Альфа срез по взаимному консонансу

Номер	Концепт	Начальное значение
1	УБИ 005	Очень низкий
2	УБИ 006	Очень низкий
3	УБИ 007	Очень низкий
4	УБИ 016	Очень низкий
5	УБИ 017	Очень низкий
6	УБИ 025	Очень низкий
7	УБИ 027	Очень низкий
8	УБИ 099	Очень низкий
9	F	Очень низкий

10.11. Экранная копия интерфейса по результатам динамического моделирования: Ввод начальных значений

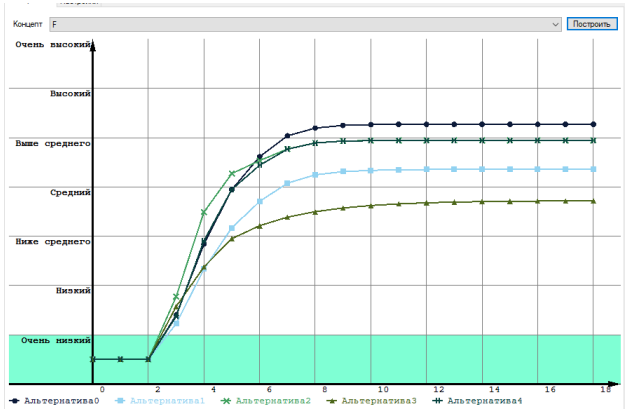
Шаг	Длительность	Объект	Действие	Значение
1	1	УБИ 005	Установить ...	Очень низкий
1	1	УБИ 006	Установить ...	Очень низкий
1	1	УБИ 025	Установить ...	Очень низкий
1	1	УБИ 027	Установить ...	Очень низкий
1	1	УБИ 099	Установить ...	Очень низкий
1	1	F	Установить ...	Очень низкий

10.12. Экранная копия интерфейса по результатам динамического моделирования: Установка значений концептов

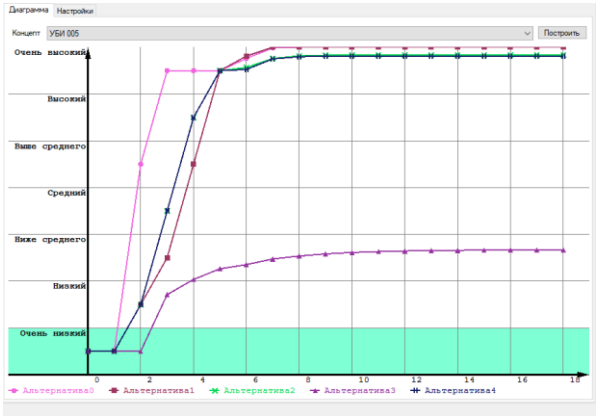


10.13. Экранная копия интерфейса по результатам динамического моделирования: Формирование альтернатив

10.14. Экранная копия интерфейса по результатам динамического моделирования: Результат моделирования по заданному сценарию



10.15. Экранная копия интерфейса по результатам динамического моделирования: Результат моделирования по целевого концепта



10.16 Экранная копия интерфейса по результатам динамического моделирования: Результат моделирования по концепту «УБИ 005»

Рисунок 10. Экранные копии интерфейсов, полученных в ходе нечеткого моделирования при работе в СППР «ИГЛА» (пример работы с нечеткой моделью)

Контрольные вопросы

1. Введите со ссылкой на источники определение категорий: модель, нечеткая модель, когнитивная модель, когнитивная карта, фактор, концепт, наблюдаемый концепт, изменяемый концепт, целевой концепт, эксперимент, событие, сценарий развития событий, статичный анализ модели, динамичный анализ модели, импульсное влияние.
2. Опишите, чем отличаются четкая модель от нечеткой (слабоструктурированной) модели.
3. Перечислите требования, предъявляемые к концептам когнитивной модели.
4. Перечислите и опишите алгоритм определения начальных условий при построении когнитивной модели.
5. Опишите методы и способы реализации когнитивной модели.
6. Каким образом можно влиять на развитие ситуации в развитии модели?
7. Каким образом в матрице межфакторного влияния численно показывается «сильное усиливающее влияние» факторов друг на друга?
8. Опишите основные этапы построения когнитивной модели.
9. Опишите возможности нечеткого моделирования в системе MentalModeler.
10. Опишите возможности нечеткого моделирования в СППР «ИГЛА».
11. Опишите как выполняется и что получается в ходе статичного анализа нечеткой модели в системе MentalModeler.
12. Опишите как выполняется и что получается в ходе статичного анализа нечеткой модели в СППР «ИГЛА».
13. Опишите как выполняется и что получается в ходе динамичного анализа нечеткой модели в системе MentalModeler.
14. Опишите как выполняется и что получается в ходе динамичного анализа нечеткой модели в СППР «ИГЛА».
15. О чем говорит отсутствие динамики (импульсного влияния) в нечеткой модели?

Источники

1. Система поддержки принятия решений "ИГЛА" [Электронный ресурс]. – Режим доступа: iipo.tu-bryansk.ru/quill/download.html?ysclid=lna9ry6fqq552527188//
2. MentalModeler [Электронный ресурс]. – Режим доступа: https://dev.mentalmodeler.com

3. Козлов, Л.А. Когнитивное моделирование на ранних стадиях проектной деятельности: учебное пособие //М-во образования и науки Российской Федерации, Федеральное агентство по образованию, ГОУВПО "Алтайский гос. технический ун-т им. И. И. Ползунова". – Барнаул : Изд-во АлтГТУ, 2009. – 245 с.

4. Федюченко, Л. Г. Когнитивное моделирование учебного и научного текста : монография // Л. Г. Федюченко. – Тюмень : ТюмГУ, 2012. – 160 с. – ISBN 978-5-400-00675-3.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 16
МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИХ СИСТЕМ. ЗАКЛЮЧИТЕЛЬНОЕ ЗАНЯТИЕ

*Время выполнения:*2 часа.

Методические указания

Работа выполняется под руководством преподавателя. Обучаемые работают за ПЭВМ, имеющих доступ в Интернет.

Ход выполнения работы

1. Подготовка к занятию: по результатам выполненных практических заданий №1-15 подготовить презентацию по следующей структуре:

Слайд 1: Титульный (оформляется по титульному листу формы отчета).

Слайд 2:

1.1. Наименование предприятия.

1.2. Организационно-правовая форма.

1.3. Сфера деятельности, отрасль, функционал.

1.4. Виды данных, обрабатываемых на предприятии.

1.5. Количество сотрудников.

Слайд 3:

1.6. Организационно-структурная схема работы предприятия с обозначением количества сотрудников в каждом структурном подразделении - представить рисунком.

Слайд 4:

1.7. Описание вида информационно-аналитической системы (класс, вид по топологии), визуализация топологической схемы ИАС предприятия (организации).

1.8. Визуализация архитектуры объекта защиты.

Слайд 5:

1.9. Анализ информационно-аналитических систем, использование которых возможно на предприятии. Представляем в виде таблицы.

Слайд 6-8 – Модель нарушителя информационной безопасности объекта защиты.

Слайд 9 – Модель угроз ИБ объекта защиты.

Слайд 10 – Модель актуальных угроз ИБ объекта защиты.

Слайд 11-15 – Моделирование развития событий ИБ на объекте защиты.

Слайд 16 – Заключение.

Слайд 17 – Заключительный слайд.

Пояснение. Количество и нумерация слайдов может не соответствовать представленной структуре, исходя из контекста слайдов.

В презентации должно быть минимума текста: только таблицы, схемы, рисунки, графики.

3. Выступить с докладом по подготовленной презентации.

4. Пройти тестирование по дисциплине. Пример тестовых заданий представлен в Приложении Б.

ЗАКЛЮЧЕНИЕ

В практикуме рассмотрены модели и методы, используемые для построения информационно-аналитических систем, во-первых, как объектов защиты; во-вторых, как систем, обеспечивающих и поддерживающих работу с объектами защиты.

В предложенном издании (практикуме) «Моделирование информационно-аналитических систем» рассмотрены практические вопросы реализации инфраструктурного, функционального, когнитивного (нечеткого) моделирования ИАС; вопросам моделирования злоумышленных воздействий на ИАС и моделирования угроз ИБ на базе регулятивного подхода, d-моделирования с использованием экспертных методов.

Объем рассмотренного материала соответствует дисциплине «Моделирование информационно-аналитических систем» для подготовки специалистов по специальности 10.05.04 – Информационно-аналитические системы безопасности».

Полученные компетенции могут быть использованы студентами для выполнения научно-исследовательских работ.

ПРИЛОЖЕНИЕ А

ПРИМЕРЫ ПРЕДСТАВЛЕНИЯ ДАННЫХ ПО ОБРАБОТКЕ И АНАЛИЗУ РЕЗУЛЬТАТОВ РАБОТЫ ЭКСПЕРТНОЙ ГРУППЫ (ОПИСАНИЕ РЕЗУЛЬТАТОВ РАБОТЫ В ОТЧЕТЕ)

К экспериментальному исследованию привлекалась экспертная группа, состоящая из 3 специалистов. Для экспертизы были предоставлены 25 угроз ИБ (*в тексте прилагается список угроз*). Эксперты представляли свое мнению по каждому из методов:

1) метод непосредственной оценки;
2) метод ранжирования;
3) метод парных сравнений.

По результатам работы экспертов получены следующие результаты.

1. Метод непосредственной оценки

Результаты работы экспертной группы по определению актуальных угроз ИБ для заданной ИАС с помощью метода непосредственной оценки представлены в табл. А.1.

Таблица А.1. Результаты работы экспертной группы по определению актуальных угроз ИБ для заданной ИАС с помощью метода непосредственной оценки

№ угрозы	Эксперт 1	Эксперт 2	Эксперт 3	Результат эксп. оценки
11	0,3	0,2	0,36	0,286667
12	0,5	0,5	0,46	0,486667
15	0,7	0,6	0,7	0,666667
23	0,9	0,8	1	**0,9**
26	0,95	0,95	0,95	**0,95**
30	0,4	0,5	0,5	0,466667
63	0,5	0,5	0,5	0,5
67	0,98	0,9	0,94	**0,94**
71	0,75	0,7	0,72	0,723333
74	1	0,9	1	**0,966667**
88	0,94	0,8	0,79	**0,843333**
89	0,3	0,4	0,4	0,366667
90	0,6	0,5	0,6	0,566667
91	0,33	0,3	0,37	0,333333
100	0,74	0,75	0,7	0,73
104	0,65	0,65	0,65	0,65

Окончание табл. А.1

№ угрозы	Эксперт 1	Эксперт 2	Эксперт 3	Результат эксп. оценки
109	0,64	0,6	0,8	0,68
139	1	1	1	**1**
113	0,25	0,2	0,32	0,256667
121	0,29	0,3	0,4	0,33
124	0,55	0,6	0,7	0,616667
125	0,89	0,9	0,9	**0,896667**
143	0,46	0,4	0,5	0,453333
145	0,82	0,85	0,9	**0,856667**
149	0,67	0,6	0,7	0,656667

На рис. А.1-А.4 выполнена графическая визуализация работы экспертов.

Рисунок А.1. Графическая визуализация результатов работы эксперта 1 с помощью метода экспертных оценок

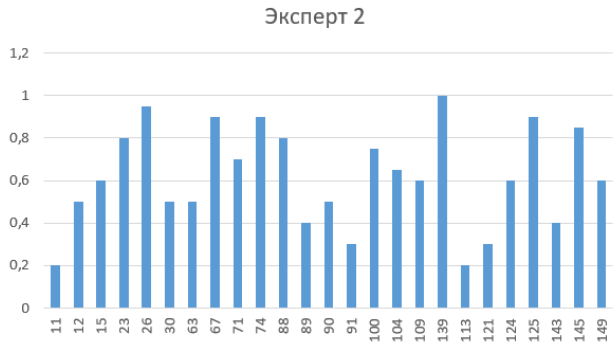


Рисунок А.2. Графическая визуализация результатов работы эксперта 2 с помощью метода экспертных оценок

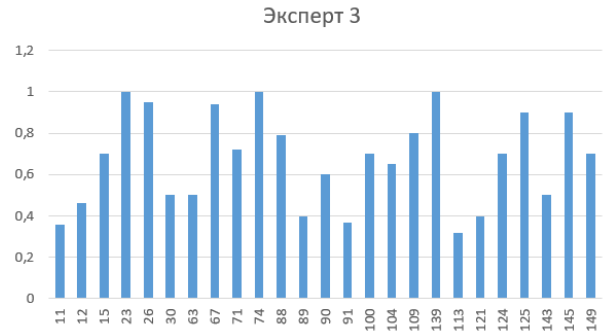


Рисунок А.3. Графическая визуализация результатов работы эксперта 3 с помощью метода экспертных оценок

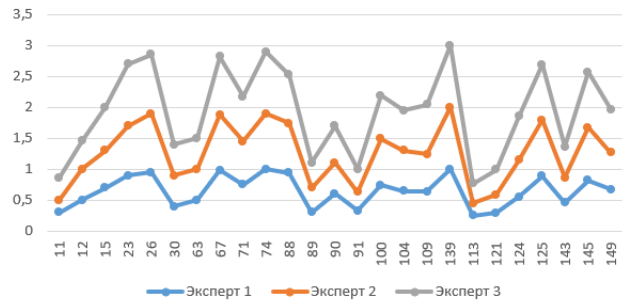


Рисунок А.4. Графическая визуализация результатов работы экспертной группы с помощью метода экспертных оценок

На рис. А.5 – визуализация результата обработки полученных экспертных данных.

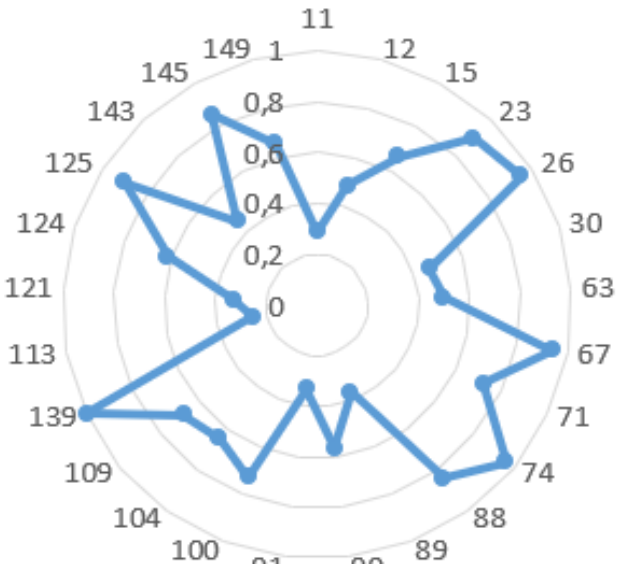


Рисунок А.5. Визуализация результата обработки полученных экспертных данных с помощью метода непосредственных оценок

По результатам анализа табл. А.1 определены 8 актуальных угроз ИБ: УБИ 139, УБИ 074, УБИ 026, УБИ 067, УБИ 023, УБИ 125, УБИ 145, УБИ 088.

Выводы:

1. Анализ результатов экспертной работы показал, что все три эксперта определили в качестве наиболее опасных практически одни и те же угрозы, с незначительными отклонениями в самих оценках.

2. В ходе экспертного исследования угроз ИБ ИАС с помощью метода непосредственной оценки в качестве актуальных определены следующие угрозы: УБИ 139, УБИ 074, УБИ 026, УБИ 067, УБИ 023, УБИ 125, УБИ 145, УБИ 088.

2. Метод ранжирования

Результаты работы экспертной группы по определению актуальных угроз ИБ для заданной ИАС с помощью метода ранжирования представлены в табл. А.2.

Таблица А.2. Результаты работы экспертной группы по определению актуальных угроз ИБ для заданной ИАС с помощью метода ранжирования

№ угрозы	Эксперт 1	Эксперт 2	Эксперт 3	Результат эксп. оценки
11	3	1	2	2
12	9	10	6	8,333333
15	15	11	13	13
23	20	18	23	20,33333

Окончание табл. А.2

№ угрозы	Эксперт 1	Эксперт 2	Эксперт 3	Результат эксп. оценки
26	22	24	22	22,66667
30	6	9	9	8
63	8	8	8	8
67	23	23	21	22,33333
71	17	16	16	16,33333
74	25	21	25	23,66667
88	21	19	17	19
89	4	5	5	4,666667
90	11	7	10	9,333333
91	5	4	3	4
100	16	17	15	16
104	13	15	11	13
109	12	12	18	14
139	24	25	24	24,33333
113	1	2	1	1,333333
121	2	3	4	3
124	10	13	12	11,66667
125	19	22	19	20
143	7	6	7	6,666667
145	18	20	20	19,33333
149	14	14	14	14

На рис. А.6-А.9 выполнена графическая визуализация работы экспертов.

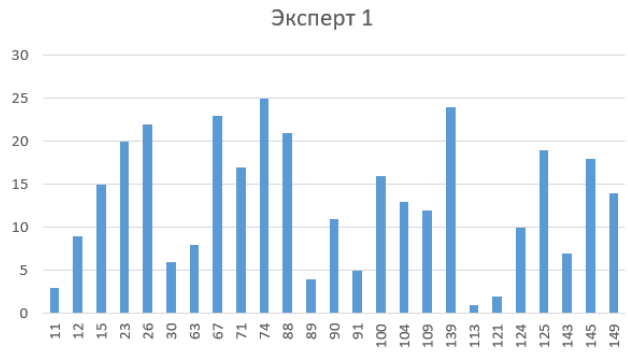


Рисунок А.6. Графическая визуализация результатов работы эксперта 1 с помощью метода ранжирования

Рисунок А.7. Графическая визуализация результатов работы эксперта 2 с помощью метода ранжирования

Рисунок А.8. Графическая визуализация результатов работы эксперта 3 с помощью метода ранжирования

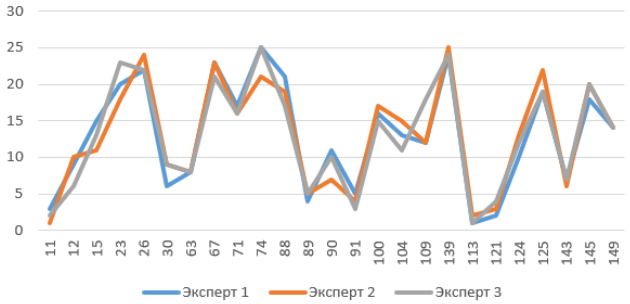


Рисунок А.9. Графическая визуализация результатов работы экспертной группы с помощью метода ранжирования

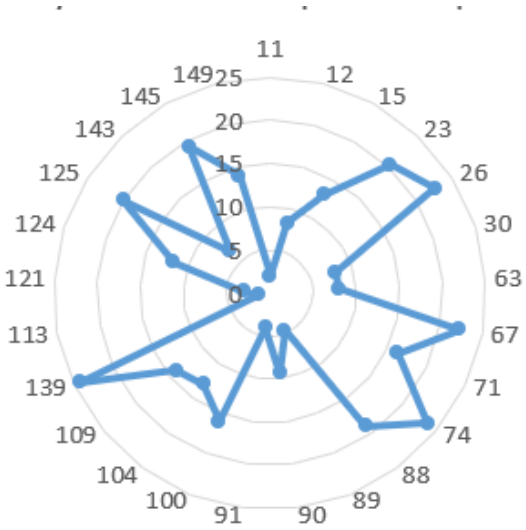


Рисунок А.10. Визуализация результата обработки полученных экспертных данных с помощью метода ранжирования

По результатам анализа табл. А.2 определены 8 актуальных угроз ИБ: УБИ 139, УБИ 074, УБИ 026, УБИ 067, УБИ 023, УБИ 125, УБИ 145, УБИ 088.

Выводы:

1. Анализ результатов экспертной работы показал, что все три эксперта определили в качестве наиболее опасных практически одни и те же угрозы, с незначительными отклонениями в самих оценках.

2. В ходе экспертного исследования угроз ИБ ИАС с помощью метода непосредственной оценки в качестве актуальных определены следующие угрозы: УБИ 139, УБИ 074, УБИ 026, УБИ 067, УБИ 023, УБИ 125, УБИ 145, УБИ 088.

3. Метод парных сравнений

Результаты работы экспертов в ходе определения актуальных угроз ИБ для заданной ИАС с помощью метода парных сравнений представлены на рис. А.11-А.13.

	11	12	15	23	26	30	63	67	71	74	88	89	90	91	100	104	109	139	113	121	124	125	143	145	149
11	0	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	2	2	1	1	1	1	1
12	2	0	1	1	1	2	0	1	1	1	1	2	1	2	1	1	1	1	2	2	1	1	1	1	1
15	2	2	0	1	1	2	2	1	1	1	1	2	2	2	1	2	2	1	2	2	2	1	2	1	2
23	2	2	2	0	1	2	2	1	2	1	2	2	2	2	2	2	2	1	2	2	2	2	2	2	2
26	2	2	2	2	0	2	2	1	2	1	2	2	2	2	2	2	2	1	2	2	2	2	2	2	2
30	2	1	1	1	1	0	1	1	1	1	2	1	2	1	1	1	1	2	2	1	1	1	1	1	1
63	2	0	1	1	1	2	0	1	1	1	1	2	1	2	1	1	1	1	2	2	1	1	2	1	1
67	2	2	2	2	2	2	2	0	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
71	2	2	2	1	1	2	2	1	0	1	1	2	2	2	2	2	2	1	2	2	2	1	2	1	2
74	2	2	2	2	2	2	2	2	2	0	2	2	2	2	2	2	2	0	2	2	2	2	2	2	2
88	2	2	2	2	1	2	2	1	2	1	0	2	2	2	2	2	2	1	2	2	2	2	2	2	2
89	0	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	2	2	1	1	1	1	1
90	2	2	1	1	1	2	2	1	1	1	1	2	0	2	1	2	2	1	2	2	2	1	2	1	1
91	2	1	1	1	1	1	1	1	1	1	1	2	1	0	1	1	1	1	2	2	1	1	1	1	1
100	2	2	2	1	1	2	2	1	1	1	1	2	2	2	0	2	1	2	2	2	2	1	2	1	2
104	2	2	1	1	1	2	2	1	1	1	1	2	2	2	1	0	2	1	2	2	2	1	2	1	1
109	2	2	1	1	1	2	2	1	1	1	1	2	2	2	1	1	0	1	2	2	2	1	2	1	1
139	2	2	2	2	2	2	2	2	2	0	2	2	2	2	2	2	2	0	2	2	2	2	2	2	2
113	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1
121	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	0	1	1	1	1	1
124	2	2	1	1	1	2	2	1	1	1	1	2	1	2	1	1	1	1	2	2	0	1	2	1	1
125	2	2	2	1	1	2	2	2	1	1	1	2	2	2	2	2	2	1	2	2	2	0	2	2	2
143	2	1	1	1	1	2	1	1	1	1	1	2	1	2	1	1	1	1	2	2	1	1	0	1	1
145	2	2	2	1	1	2	2	1	2	1	1	2	2	2	2	2	2	1	2	2	2	1	2	0	2
149	2	2	1	1	1	2	2	1	1	1	1	2	2	2	1	2	2	1	2	2	2	1	2	1	0

Рисунок А.11. Результаты работы эксперта 1 по определению актуальных угроз ИБ для заданной ИАС с помощью метода парных сравнений

	11	12	15	23	26	30	63	67	71	74	88	89	90	91	100	104	109	139	113	121	124	125	143	145	149
11	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
12	2	0	1	1	1	0	0	1	1	1	1	2	0	2	1	1	1	1	2	2	1	1	2	1	1
15	2	2	0	1	1	2	2	1	1	1	1	2	2	2	1	1	0	1	2	2	0	1	2	1	0
23	2	2	2	0	1	2	2	1	2	1	0	2	2	2	2	2	2	1	2	2	2	1	2	1	2
26	2	2	2	2	0	2	2	2	2	2	2	2	2	2	2	2	2	1	2	2	2	2	2	2	2
30	2	0	1	1	1	0	0	1	1	1	1	2	0	2	1	1	1	1	2	2	1	1	2	1	1
63	2	0	1	1	1	0	0	1	1	1	1	2	0	2	1	1	1	1	2	2	1	1	2	1	1
67	2	2	2	2	1	2	2	0	2	0	2	2	2	2	2	2	2	1	2	2	2	0	2	2	2
71	2	2	2	1	1	2	2	1	0	1	1	2	2	2	2	2	2	1	2	2	2	1	2	1	2
74	2	2	2	2	1	2	2	2	2	0	2	2	2	2	2	2	2	0	2	2	2	2	2	2	2
88	2	2	2	1	1	2	2	1	2	1	0	2	2	2	2	2	2	1	2	2	2	1	2	1	2
89	2	1	1	1	1	1	1	1	1	1	1	0	1	2	1	1	1	1	2	2	1	1	0	1	1
90	2	0	1	1	1	0	2	1	1	1	1	2	0	2	1	1	1	1	2	2	1	1	2	1	1
91	2	1	1	1	1	1	2	1	1	1	1	1	1	0	1	1	1	1	2	0	1	1	1	1	1
100	2	2	2	1	1	2	2	1	2	1	1	2	2	2	0	2	1	2	2	2	2	1	2	1	2
104	2	2	2	1	1	2	2	1	1	1	1	2	2	2	1	0	2	1	2	2	2	1	2	1	2
109	2	2	0	1	1	2	2	1	1	1	1	2	2	2	1	1	0	1	2	2	0	1	2	1	0
139	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	0	2	2	2	2	2	2	2
113	0	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1
121	2	1	1	1	1	1	2	1	1	1	1	1	1	0	1	1	1	1	2	0	1	1	1	1	1
124	2	2	0	1	1	2	2	1	1	1	1	2	2	2	1	1	0	1	2	2	0	1	2	1	0
125	2	2	2	2	1	2	2	0	2	0	2	2	2	2	2	2	2	1	2	2	2	0	2	2	2
143	2	1	1	1	1	1	2	1	1	1	1	0	1	2	1	1	1	1	2	2	1	1	0	1	1
145	2	2	2	2	1	2	2	1	2	1	2	2	2	2	2	2	2	1	2	2	2	1	2	0	2
149	2	2	0	1	1	2	2	1	1	1	1	2	2	2	1	1	0	1	2	2	0	1	2	1	0

Рисунок А.12. Результаты работы эксперта 2 по определению актуальных угроз ИБ для заданной ИАС с помощью метода парных сравнений

	11	12	15	23	26	30	63	67	71	74	88	89	90	91	100	104	109	139	113	121	124	125	143	145	149
11	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1
12	2	0	1	1	1	1	1	1	1	1	1	2	1	2	1	1	1	1	2	2	1	1	1	1	1
15	2	2	0	1	1	2	2	1	1	1	1	2	2	2	0	2	1	1	2	2	0	1	2	1	0
23	2	2	2	0	2	2	2	2	2	0	2	2	2	2	2	2	2	0	2	2	2	2	2	2	2
26	2	2	2	1	0	2	2	2	2	1	2	2	2	2	2	2	2	1	2	2	2	2	2	2	2
30	2	2	1	1	1	0	0	1	1	1	1	2	1	2	1	1	1	1	2	2	1	1	0	1	1
63	2	2	1	1	1	0	0	1	1	1	2	1	2	1	1	1	1	1	2	2	1	1	0	1	1
67	2	2	2	1	1	2	2	0	2	1	2	2	2	2	2	2	2	1	2	2	2	2	2	2	2
71	2	2	2	1	1	2	2	1	0	1	1	2	2	2	2	2	2	1	1	2	2	2	1	2	1	2
74	2	2	2	0	2	2	2	2	2	0	2	2	2	2	2	2	2	0	2	2	2	2	2	2	2
88	2	2	2	1	1	2	2	1	2	1	0	2	2	2	2	2	2	1	1	2	2	2	1	2	1	2
89	2	1	1	1	1	1	1	1	1	1	1	0	1	2	1	1	1	1	2	0	1	1	1	1	1
90	2	2	1	1	1	2	2	1	1	1	1	2	0	2	1	1	1	1	2	2	1	1	2	1	1
91	2	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	2	1	1	1	1	1	1
100	2	2	1	1	1	2	2	1	1	1	1	2	2	2	0	2	1	2	2	2	0	1	2	1	2
104	2	2	1	1	1	2	2	1	1	1	1	2	2	2	1	0	2	1	2	2	2	1	2	1	1
109	2	2	2	1	1	2	2	1	2	1	2	2	2	2	2	1	0	1	2	2	2	1	2	1	2
139	2	2	2	0	2	2	2	2	2	0	2	2	2	2	2	2	2	0	2	2	2	2	2	2	2
113	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1
121	2	1	1	1	1	1	1	1	1	1	1	0	1	2	1	1	1	1	2	0	1	1	1	1	1
124	2	2	0	1	1	2	2	1	1	1	1	2	2	2	0	2	1	1	2	2	0	1	2	1	0
125	2	2	2	1	1	2	2	1	2	1	2	2	2	2	2	2	2	1	2	2	2	0	2	0	2
143	2	2	1	1	1	0	0	1	1	1	1	2	1	2	1	1	1	1	2	2	1	1	0	1	1
145	2	2	2	1	1	2	2	1	2	1	2	2	2	2	2	2	2	1	2	2	2	0	2	0	2
149	2	2	0	1	1	2	2	1	1	1	1	2	2	2	0	2	1	1	2	2	0	1	2	1	0

Рисунок А.13. Результаты работы эксперта 1 по определению актуальных угроз ИБ для заданной ИАС с помощью метода парных сравнений

Результаты обработки результатов работы экспертной группы по определению актуальных угроз ИБ для заданной ИАС с помощью метода парных оценок представлены на рис. А.14-А.15.

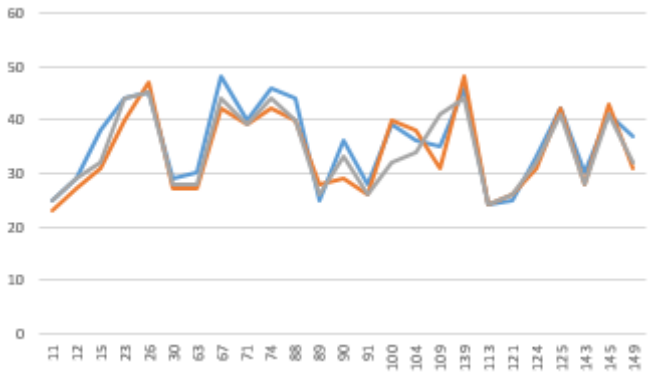


Рисунок А.14. Графическая визуализация результатов работы экспертной группы с помощью метода парных сравнений

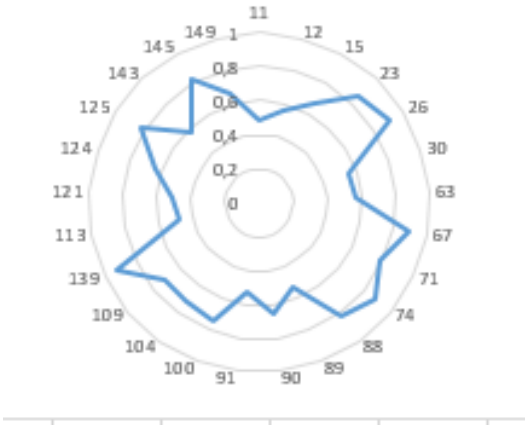


Рисунок А.15. Визуализация результата обработки полученных экспертных данных с помощью метода парных сравнений

В ходе анализа результатов работы экспертов с помощью метода парных сравнений в качестве актуальных определены следующие угрозы ИБ ИАС: УБИ 139, УБИ 026, УБИ 067, УБИ 074, УБИ 023, УБИ 125, УБИ 145, УБИ 088.

Выводы: аналогичны выводам, полученным по результатам работы методов непосредственной оценки и ранжирования.

4. Анализ результатов работы экспертной группы по определению актуальных угроз ИБ ИАС

Результаты работы экспертов в ходе определения актуальных угроз ИБ для заданной ИАС по каждому из используемых методов представлены на рис. А.16-А.19.

Рисунок А.16. Результаты работы эксперта 1 в ходе определения актуальных угроз ИБ для заданной ИАС по каждому из используемых методов

Рисунок А.17. Результаты работы эксперта 2 в ходе определения актуальных угроз ИБ для заданной ИАС по каждому из используемых методов

Рисунок А.18. Результаты работы эксперта 3 в ходе определения актуальных угроз ИБ для заданной ИАС по каждому из используемых методов

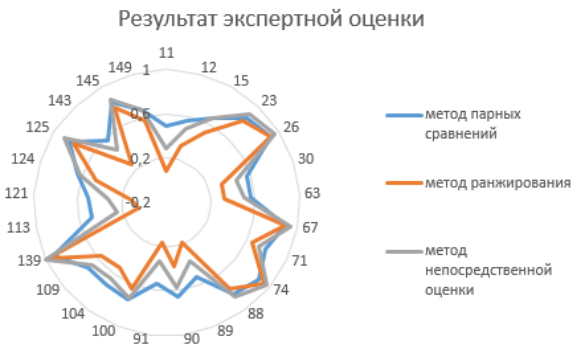


Рисунок А.19. Визуализация результатов обработки полученных экспертных данных по каждому из используемых методов

По результатам полученных данных определено следующее.

1. В ходе исследования угроз ИБ ИАС с помощью методов непосредственной оценки, ранжирования и парных сравнений в качестве актуальных определены следующие угрозы: УБИ 139, УБИ 074, УБИ 026, УБИ 067, УБИ 023, УБИ 125, УБИ 145, УБИ 088. Полученные результаты по используемым методам идентичны, что говорит о точности полученных результатов.

2. В качестве наиболее вероятной определена угроза УБИ139 в результате работы всех трех методов. Остальные угрозы из полученного списка актуальных угроз меняют в списке свои позиции, но не критично.

3. Угрозы ИБ ИАС, не входящие в полученный список актуальных угроз, по своей значимости (согласно мнений экспертов) имеют не значительные отклонения от результирующей оценки (см. рис. А.19).

ПРИЛОЖЕНИЕ Б

ПРИМЕР ТЕСТОВЫХ ЗАДАНИЙ

1. Информационно-аналитическая система – это особый класс информационных систем, предназначенных для:

а) аналитической обработки данных;

б) принятия решений в сфере ИБ;

в) получения справок и отчетов;

г) реализации политики безопасности в организации.

2. Архитектура современной ИАС включает:

а) транзакционные базы данных;

б) хранилища данных;

в) аналитические базы данных.

г) витрины данных;

д) инструменты интеллектуального и делового анализа данных;

е) Web-портал.

3. В информационно-аналитической системе реализуются следующие виды схем данных:

а) звезда;

б) снежинка;

в) шина;

г) созвездие.

4. На каком этапе производится разработка сценариев развития событий?

а) на этапе принятия решения;

б) на этапе проектирования;

в) на этапе планирования;

г) на этапе моделирования.

5. Для оценки инструментов обработки данных в ИАС используют следующие критерии:

а) технические характеристики;

б) скорость внедрения;

в) уместность использования в каждом конкретном случае;

г) стоимостные характеристики

д) все вышеперечисленное.

6. Как называется математическая модель, которая учитывает процессы внутри блока и межэлементные связи?

а) полная модель;

б) макромодель;

в) микромодель;

г) частичная модель.

7. Что представляет собой система автоматизированного проектирования (САПР)?

а) средство автоматизации проектирования;

б) система деятельности людей по проектированию объектов;

в) система сбора информации;

г) средство обработки данных.

8. Архитектура современной информационно-аналитической системы не реализуется на уровне:

а) сбора и первичная обработки данных;

б) извлечения, преобразования и загрузки данных;

в) складирования данных;

г) представления данных в витринах данных;

д) анализа данных;

е) Web-портала;

ж) оптимизации данных.

9. Разработана технологическая модель технологического процесса. Чем она является?

а) объектом проектирования;

б) объектом автоматизации проектирования;

в) субъектом взаимодействия;

г) объектом для реализации.

10. Чем определяется экономичность математических моделей?

а) затратами машинного времени;

б) возможностью использования для анализа информационного процесса и его элементов;

в) требованиями высокой точности;

г) требованием заказчика.

11. Математические модели – это:

а) факторные модели;

б) физические модели;

в) формальные модели;

г) технические модели;

д) экспериментальные модели.

12. Необходимо построить математическую модель технологического процесса производства. Какой подход необходимо использовать?

а) статистический подход;

б) семантический подход;

в) прагматический подход;

г) футуристический подход;

д) экспертный подход.

13. Какие характеристики рассчитываются при построении математической модели как результата пассивного эксперимента?

а) оценка математического ожидания;

б) оценка среднеквадратического отклонения;

в) переходные характеристики;

г) входные характеристики.

14. В ходе НИР для системы менеджмента производимой продукции разработана математическая модель в виде системы уравнений регрессии. К какому этапу жизненного цикла можно отнести полученный результат?

а) этап функционального проектирования;

б) этап конструкторского проектирования;

в) этап технологической подготовки производства;

г) этап управления проектными данными.

15. На управляемом динамическом производстве выполняются следующие последовательные этапы:

а) принятие решения;

б) оценка конструкции;

в) технологическое проектирование;

г) верификация;

д) все выше обозначенное.

16. Чем характеризуется адекватность математической модели?

а) размерами области адекватности;

б) числом учитываемых параметров;

в) особенностями выбранных моделей;

г) адекватностью объекта моделирования;

д) алгоритмом ее реализации.

17. Риск информационной безопасности - это:

а) возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации;

б) вероятность возникновения убытков или неполучения доходов по сравнению с прогнозируемым вариантом;

в) упущенная выгода;

г) комплексный показатель надежности элементов техносферы, который выражает вероятность возникновения аварии или катастрофы при эксплуатации машин, механизмов, реализации технологических процессов, строительстве и эксплуатации зданий и сооружений.

18. Нечеткая когнитивная модель для объекта моделирования позволяет:

а) прогнозировать основные выходные характеристики;

б) получить статистические характеристики;

в) получить экономические характеристики;

г) исследовать варианты структуры процесса;

д) все выше перечисленное.

19. Активный аудит – это…

а) исследование средств для определения соответствия их решениям задач информационной безопасности;

б) исследование состояние системы сетевой защиты, использование которой помогает хакеру проникнуть в сети и нанести урон компании;

в) исследование состояния защищенности информационной системы с точки зрения хакера (или некоего злоумышленника, обладающего высокой квалификацией в области информационных технологий);

г) набор адекватных контрмер, осуществляемых в ходе управления рисками;

д) все выше перечисленное.

20. Для визуализации блоков функциональной модели в нотации IDEF0 установлены следующие синтаксические правила:

а) размеры блоков должны быть достаточными для того, чтобы включить имя и номер блока;

б) блоки должны быть прямоугольными, с прямыми углами;

в) блоки должны быть нарисованы сплошными линиями;

г) все выше перечисленное.

21. Связь параметров технологического процесса и показателей качества системы определяется формализованной моделью, реализованной в:

а) СППР;

б) САПР ТП;

в) АСУ ТП;

г) СЗИ;

д) OLAP-системе

22. Описание объектов и связей между ними выполняется на уровне:

а) концептуальной модели;

б) логической модели;

в) физической модели;

г) технологической модели.

23. На какой стадии выдается окончательная конструкторская документация при проектировании информационно-аналитической системы?

а) техническое задание на проектируемый объект;

б) научно-исследовательская работа;

в) эскизный проект;

г) технический проект;

д) рабочий проект.

24. С помощью имитационной модели не возможно оценить:

а) показатели качества;

б) время реализации процесса;

в) техническую производительность;

д) иное.

25. Задано множество конечных результатов прогнозируемых вариантов решений задачи. Для выбора варианта структуры в данном случае каким алгоритмом можно воспользоваться?

а) дискретного линейного программирования;

б) динамического программирования;

в) быстрой сортировки;

г) эвристических приемов.

26. Для моделирования рисков информационной безопасности можно использовать методики:

а) Windows, RISK WATCH, КОНДОР;

б) ГРИФ, RISK WATCH, КОНДОР;

в) RISK WATCH, КОНДОР, АСТРА;

г) ГРИФ, RISK WATCH, Comodo Internet Security;

д) экспертной оценки; SWOT.

27. Какая модель строится в результате применения принципа «черного ящика»?

а) технологическая модель;

б) физико-топологическая модель;

в) неориентированный граф;

г) имитационная модель.

28. Современные виды систем принятия решений не наделены следующими возможностями:

а) формирование статистики и ее проверка;

б) составление трендовых прогнозов;

в) планирование и контроль качества;

г) финансовый анализ и прогнозирование;

д) вынести предложение, какое решение принять.

29. Чем определяется адекватность математических моделей?

а) затратами машинного времени;

б) возможностью использования для анализа технологического процесса и его элементов;

в) требованиями высокой точности;

г) сложностью алгоритма.

30. В ходе когнитивного моделирования выполняется построение:

а) когнитивной карты;

б) «черного ящика»;

в) алгоритма;

г) матрицы межфакторного влияния.

31. Для моделирования рисков информационной безопасности необходимо:

а) оценить систему управления ИБ;

б) определить вероятности реализации угроз;

в) разработать модель злоумышленника информационной безопасности;

г) разработать политику информационной безопасности организации;

д) сформировать экспертную группу.

32. Риск информационной безопасности от реализации 10 актуальных угроз, значения вероятностей которых равны 0,3, стоимость возможного ущерба от реализации каждой угрозы – 1000 усл. ед. равен:

а) 3000 усл.ед.;

б) 3000 рублей;

в) 1003 усл. ед.;

г) 500 усл. ед..

33. В процессе продвижения данных в информационное хранилище используются следующие критерии оценки качества данных по структурному представлению:

а) по критичности ошибок в данных – ошибки в именах полей, типах данных;

б) по правильности форматов и представлений данных;

в) на соответствие ограничениям целостности;

г) на кроссязыковый разрыв;

д) уникальности внутренних и внешних ключей;

е) по полноте данных и связей.

34. Надежность модели – это:

а) внутренний параметр;

б) внешний параметр;

в) выходной параметр;

г) показатель качества модели.

35. Эффективность модели – это:

а) внутренний параметр;

б) внешний параметр;

в) выходной параметр;

г) показатель качества модели.

36. На безопасность информационно-аналитической системы оказывает влияние:

а) наличие механизмов защиты и возможность их использования;

б) стойкость существующих механизмов защиты;

в) реализация мероприятий политики безопасности организации;

г) все выше обозначенное.

37. Проведение комплексного внешнего аудита предприятия с последующей сертификацией демонстрирует его контрагентам:

а) способность предприятия выступать в качестве надежного партнера, которому можно доверить конфиденциальные сведения;

б) полное отсутствие уязвимостей в системах и сетях;

в) достаточную страховую защиту от информационных рисков;

г) конкурентоспособность на рынке товаров и услуг;

д) все выше перечисленное.

38. Сертификация системы безопасности на соответствие требованиям стандарта ISO 17799 может быть осуществлена по результатам:

а) внешнего аудита;

б) внутреннего аудита;

в) инструментальной проверки защищенности;

г) контроля качества;

д) мониторинга информационной безопасности;

е) все выше перечисленное.

39. Аудит информационной безопасности подразделяется на:

а) текущий и итоговый;

б) внешний и внутренний;

в) объективный и субъективный;

г) активный и пассивный;

д) промежуточный.

40. Инициаторами аудита информационной безопасности могут выступать:

а) государственные структуры;

б) органы стандартизации;

в) руководители предприятия;

г) специалист по защите информации;

д) конкуренты.

41. Цели аудита информационной безопасности могут включать в себя:

а) выявление лиц, нарушающих требования информационной безопасности;

б) сертификацию на соответствие общепризнанным требованиям и стандартам;

в) установление степени защищенности информационных ресурсов;

г) лицензирование;

д) моделирование системы защиты.

42. Использование методов математического моделирования позволяет решить задачи:

а) оптимизации системы;

б) исследования системы;

в) оценки защищенности объекта информатизации;

г) все вышеперечисленное.

43. Q-модель – это:

а) математический (абстрактный) объект, содержащий один или несколько приборов (каналов) и накопитель, в котором находятся заявки, образующие очередь и ожидающие обслуживания;

б) математический (абстрактный) объект, содержащий один или несколько приборов (каналов), обслуживающих заявки, поступающие в систему, и накопитель, в котором находятся заявки, образующие очередь и ожидающие обслуживания;

в) объект, содержащий один или несколько приборов (каналов), обслуживающих заявки, поступающие в систему, и накопитель;

г) математический (абстрактный) объект, определяющий качество обслуживания заявок в системе.

д) процессная модель, элементами которой являются объекты, полученные в результате декомпозиции исходной задачи и описанные на языке теории массового обслуживания, а также связи между ними.

44. Система массового обслуживания M/M/1 представлена:

а) одноканальной СМО с накопителем неограниченной ёмкости, в которую поступает однородный поток заявок с экспоненциальным распределением интервалов времени между последовательными заявками (простейший поток) и экспоненциальной длительностью обслуживания заявок в приборе;

б) одноканальной СМО с накопителем ограниченной ёмкости, в которую поступает однородный поток заявок с экспоненциальным распределением интервалов времени между последовательными заявками (простейший поток) и экспоненциальной длительностью обслуживания заявок в приборе;

в) многоканальной СМО с накопителем неограниченной ёмкости, в которую поступает однородный поток заявок с экспоненциальным распределением интервалов времени между последовательными заявками (простейший поток) и экспоненциальной длительностью обслуживания заявок в приборе;

г) одноканальной СМО с накопителем неограниченной ёмкости, в которую поступает однородный поток заявок с равномерным распределением интервалов времени между последовательными заявками и экспоненциальной длительностью обслуживания заявок в приборе.

45. Установите соответствие между категориями и их определениями:

1	Риск ИБ	а	совокупность руководящих принципов, правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности
2	Политика безопасности	б	модель компьютерной системы;; критерии, принципы или целевые функции защищенности и угроз формализованные правила, алгоритмы, механизмы безопасного функционирования компьютерной системы
3	Модель безопасности	в	возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации
4	Защищенность информационной системы	г	

Формат ответа: 1,x; 2,y…..

46. Установите соответствия между решаемой задачей и методами и подходами для ее реализации:

1	Построение модели нарушителя ИБ	а	Регулятивный подход
2	Построение модели угроз ИБ	б	Методы экспертных оценок
3	Оценка рисков ИБ	в	Q-моделирование
4	Оптимизация ИАС	г	Когнитивное моделирование
5	Оценка эффективности функционирования ИАС	д	Риск-ориентированный подход

Формат ответа: 1,х; 2,у…..

47. Установите соответствие между видами моделей и их недостатками:

1	многоуровневые модели безопасности	а	невозможность учета индивидуальных особенностей субъекта
2	матричных моделей безопасности	б	отсутствие контроля за потоками информации
3	дискретных моделей политики безопасности	в	статичность
4	модели конечных состояний политики безопасности	г	сложность реализации
5	модели политики безопасности на основе анализа угроз системе	д	изначальное допущение вскрываемости системы

Формат ответа: 1,х; 2,у…..

48. Дан перечень факторов:

F1 – Злоумышленные воздействия;

F2 – Масштабность и уровень производственной деятельности организации;

F3 – Количество служащих;

F4 – Возможности для технического развития предприятия;

F5 – Темпы развития предприятия в отрасли;

F6 – Динамика продаж и процентный охват рынка;

F7 – Зоны стратегического влияния;

F8 – Конкурентная способность товаров и услуг;

F9 – Уровень финансовой рентабельности, платежеспособность,

F10 – Деловая активность и привлекательность для инвестиционных вложений;

F11 – Наличие объектов и субъектов для специальной охраны – обладатели коммерческой или государственной тайны, взрывоопасные и пожароопасные участки, экологически вредное производство;

F12 – Присутствие криминальной среды;

F13 – Качество политики безопасности предприятия;

F14 – Требования нормативных, методических и организационно-распорядительных документов по обеспечению ИБ;

F15 – Доступность основных активов;

F16 – Компетентность сотрудников;

F17 – Температура окружающей среды.

Задание 1: составить перечень концептов когнитивной модели «Оценка информационной безопасности предприятия».

Задание 2: составить перечень управляемых концептов когнитивной модели «Оценка информационной безопасности предприятия».

Задание 3: составить перечень внешних факторов.

49. Дана матрица межфакторного влияния когнитивной модели:

	S1	S2	S3	S4	S5	S6
S1		0.1			0.2	
S2				-0.4		
S3		0.1				-0.15
S4			-0.4		0.6	
S5	0.3					0.2
S6		-0.7		-0.9		

Задание 1: составить перечень межэлементных положительных связей. Формат ответа Sij.

Задание 2: составить перечень межэлементных отрицательных связей. Формат ответа Sij.

Задание 3: указать наиболее сильный фактор положительного влияния, отрицательного влияния. Формат ответа Si.

50. Задана таблица значений возможного ущерба от реализации угроз ИБ информационно-аналитической системы и стоимость возможного ущерба от реализации угроз ИБ ИАС:

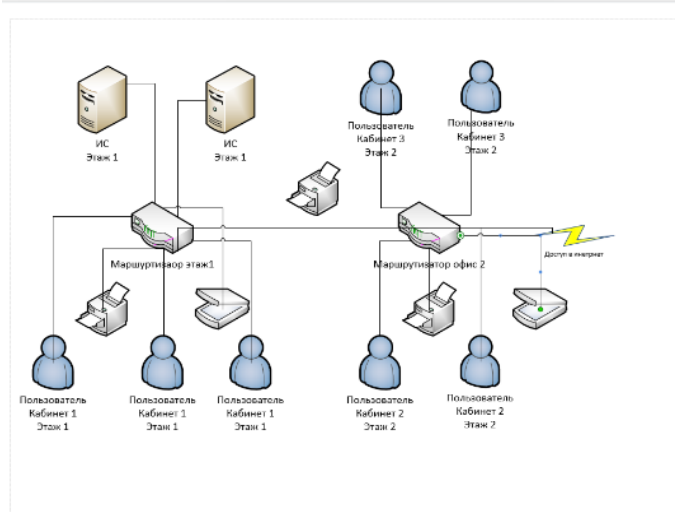
№	Обозначение угрозы ИБ	Вероятность реализации угрозы ИБ	Стоимость возможного ущерба от реализации угроз ИБ информационной системы, тыс.у.е.
1	U1	0.2	200
2	U2	0.4	257
3	U3	0.15	300
4	U4	0.9	132
5	U5	0.3	159
6	U6	0.2	425

Задание 1: С помощью двухфакторной модели определить частные риски от реализации угроз ИБ

Задание 2: С помощью двухфакторной модели определить риск ИБ

Задание 3: Указать угрозы ИБ, при реализации которых риск ИБ будет максимальным и минимальным.

51. Задана типовая архитектура ИАС предприятия:



Для ИАС, обеспечивающей функционирование данной ИАС:

Задание 1: Используя требования ФСТЭК России, разработать структуру модели угроз ИБ ИАС.

Задание 2: Используя банк данных угроз безопасности ФСТЭК России (ресурс БДУ - Вход (fstec.ru)) представить список угроз несанкционированного доступа к данным в ИАС (не более 6).

Задание 3. По результатам выполнения задания 6 разработать модель угроз НСД к данным в ИС в виде дерева угроз.

Задание 4. Сформировать список факторов влияния на реализацию технологических процессов обработки информации в специальных ИАС (не более 4).

Задание 5. Используя результаты задачи 3, на базе СППР «ИГЛА» или MentalModeler разработать когнитивную модель «Оценка защищенности данных в ИС». Количество концептов – не более 4.

Задание 6. Для модели по результатам задачи 4, используя СППР «ИГЛА» или MentalModeler выполнить статический анализ разработанной в задаче 4 модели.

52. В ходе _____ информационной безопасности выполняется оценка текущего состояния системы информационной безопасности.

53. Топологическая модель относится к классу _____ моделей.

54. С позиций когнитивного подхода процесс моделирования можно представить в виде схемы процесса моделирования, элементами которой могут являться _____.

55. Элементы когнитивной модели называются _____.

56. На этапе _____ научного проекта производится отчетность и документирование результатов.

57. Без функции _____ модель IDEF0 не имеет смысла.

58. Детализация блока на составляющие называется _____.

59. Модель в нотации IDEF0 является _____ моделью.

60. _____ диаграмма – это диаграмма, которая содержит родительский блок.

61. В IDEF0 диаграмме, небольшая ломаная (волнистая) линия, используемая для соединения метки с конкретным сегментом стрелки или примечания модели с компонентом диаграммы называется _____.

62. В когнитивной модели, для моделирования ситуаций развития событий, на один из концептов модели подается _____.

63. Краткая формулировка причины создания модели называется _____.

64. Компьютерные автоматизированные системы, целью которых является помощь людям, принимающим решение в сложных условиях, для полного и объективного анализа предметной деятельности относятся к классу систем_____.

65. Систему, способную изменять свое состояние или окружающую ее среду, называют _____.

66. Для оценки рисков ИБ достаточно, (указать количество) _____ факторов.

67. Совокупность руководящих принципов, правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности Политика безопасности организации называется _____.

68. Формальное представление политики безопасности называется _____ безопасности.

69. Сложная система — это система, состоящая из множества _____ составляющих (подсистем).

Сведения об авторах

Максимова Елена Александровна, доктор технических наук, доцент, профессор кафедры КБ-2 «Информационно-аналитические системы кибербезопасности» РТУ МИРЭА