МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Поволжский государственный университет сервиса» (ФГБОУ ВО «ПВГУС»)

Высшая школа интеллектуальных систем и кибертехнологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б.1.О.02.03 «Управление информационной безопасностью»

Направление подготовки:
10.04.01 «Информационная безопасность»

Направленность (профиль):
«Информационная безопасность интеллектуальных и информационно-аналитических систем»

Квалификация выпускника: **магистр**

Тольятти 2022

Рабочая программа дисциплины *«Управление информационной безопасностью»* разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования – *магистратура* по направлению подготовки *10.04.01 «Информационная безопасность»*, утвержденным приказом Министерства науки и высшего образования Российской Федерации от 26 ноября 2020 г. №1455

Составители:

д. э. н., профессор	Л.В. Глухова
(ученая степень, ученое звание)	(ФИО)

РПД обсуждена на заседании высшей школы интеллектуальных систем и кибертехнологий «02» 12 2022г., протокол № 4

Директор высшей школы интеллектуальных систем и кибертехнологий	к. э. н., доцент	/О.А. Филиппова
	(уч.степень, уч.звание)	(ФИО)

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Цель освоения дисциплины

Целью освоения дисциплины является:

– формирование у обучающихся общепрофессиональных компетенций, направленных на решение задач профессиональной деятельности;

– развитие навыков профессиональной деятельности;

– формирование у обучающихся универсальных компетенций, *направленных на развитие навыков системного и критического мышления*.

1.2. Перечень планируемых результатов обучения по дисциплине

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения по дисциплине**	**Основание (ПС)** *для профессиональных компетенций
УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	ИУК-3.2. Осуществляет принятие исполнительских решений в условиях спектра мнений, определение порядка выполнения заданий	**Знает:** основные функции организации и управления работой команды исполнителей **Умеет:** планировать стратегию членов команды по обеспечению информационной безопасности **Владеет:** навыками принятия исполнительских решений в условиях спектра мнений и порядка выполнения работ по управлению информационной безопасностью	
ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ИОПК-1.1. Понимает принципы, требования и структуру системы обеспечения информационной безопасности и защиты информации ИОПК-1.2. Проектирует техническое задание на создание системы обеспечения информационной безопасности и защиты информации	**Знает:** принципы обеспечения информационной безопасности и защиты информации и требования нормативных документов для разработки проекта технического задания **Умеет:** разрабатывать техническое задание на создание системы обеспечения информационной безопасности и защиты информации **Владеет:** навыками проектирования систем обеспечения информационной безопасности	
ОПК-3. Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	ИОПК-3.1. Применяет нормативные правовые акты, методические документы при подготовке распорядительных документов по обеспечению информационной безопасности, в том числе при разработке ИАС ИОПК-3.2. Разрабатывает проекты организационно-распорядительных документов по обеспечению информационной безопасности	**Знает:** принципы проектирования и разработки организационно-распорядительных документов по обеспечению информационной безопасности и требования нормативной базы ФСТЭК **Умеет:** разрабатывать проекты информационно-аналитических систем и организационно-распорядительных документов по обеспечению информационной безопасности **Владеет:** навыками работы с нормативными документами ФСТЭК при управлении информационной безопасностью	

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина относится к обязательной части Блока 1. Дисциплины (модули) программы магистратуры (Б1.О.02 Общепрофессиональный модуль).

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1. Объем и структура дисциплины

Общая трудоёмкость дисциплины составляет **3 з.е. (108 час.)**, их распределение по видам работ и семестрам представлено в таблице.

Виды учебных занятий и работы обучающихся	Трудоемкость, час
Общая трудоемкость дисциплины, час	**108**
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего), в т.ч.:	**32/8**
занятия лекционного типа (лекции)	12/ 4
занятия семинарского типа (семинары, практические занятия, практикумы, коллоквиумы и иные аналогичные занятия)	20 /4
лабораторные работы	- /-
Самостоятельная работа всего, в т.ч.:	**49/ 91**
Самоподготовка по темам (разделам) дисциплины	-/ -
Выполнение курсового проекта /курсовой работы	-/ -
Контроль (экзамен)	**27 /9**
Промежуточная аттестация	**Экзамен**

Примечание: -/- *объем часов соответственно для очной и очно-заочной форм обучения*

Дисциплина реализуется посредством проведения контактной работы с обучающимися(включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

В процессе освоения дисциплины может применяться электронное обучение и дистанционные образовательные технологии.

В процессе освоения дисциплины обучающиеся обеспечены доступом к электронной информационно-образовательной среде и электронно-библиотечным системам.

3.2. Содержание дисциплины, структурированное по темам

Планируемые результаты освоения: код формируемой компетенции и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы			Формы текущего контроля (наименование оценочного средства)
		Контактная работа		Самостоятельная работа, час	
		Лекции, час	Практические занятия, час		
УК-3; ИУК-3.2; ОПК-1; ИОПК1-1; ИОПК1-2;	**Тема 1. Основные понятия науки об управлении. Системный, процессный, нормативный подходы** 1. Системный и процессный подходы к проектированию и разработки систем управления информационной безопасностью (СУИБ) 2. Стандартизация в области построения СУИБ. Доктрина ИБ. Требования ФСТЭК 3. Политика в области управления информационной безопасностью 4. Методика анализа рисков информационной безопасности	2/2			Доклад/ сообщение
	Практическое занятие № 1. Изучение нормативной базы документов в области ИБ.		5/1		Выполнение практической работы
	Практическая работа № 2. Изучение методики оценки рисков информационной безопасности.		5/1		Выполнение практической работы
	Самостоятельная работа			16/30	Выполнение самостоятельной работы
ОПК-1; ИОПК1-1; ИОПК1-2; ОПК-3; ИОПК3.1; ИОПК-3.2;	**Тема 2. Проектирование системы управления информационной безопасностью на предприятии** 1.Разработка ТЗ на СУИБ. Проектирование состава организационных и технических мер обеспечения СУИБ 2. Планирование ресурсов для управления проектом по разработке СУИБ на предприятии 3. Моделирование проектного управления СУИБ с учетом ключевых показателей эффективности основных бизнес-процессов	4/1			Доклад/ Сообщение.
	Практическое занятие № 3. Построение функциональной модели процессов обеспечения информационной безопасности с помощью графических нотаций и в соответствии с требованиями ТЗ.		5/1		Выполнение практической работы
	Самостоятельная работа			16/30	Выполнение самостоятельной работы
УК-3; ИУК-3.2; ОПК-1; ИОПК1-1; ИОПК1-2;	**Тема 3. Оценка рисков информационной безопасности на предприятии** 1.Методика составления модели угроз и анализа рисков. Разновидности задач и проблемы 2. Программно-инструментальные средства аудита информационной безопасности	6/1			

Планируемые результаты освоения: код формируемой компетенции и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы			Формы текущего контроля (наименование оценочного средства)
		Контактная работа		Самостоятельная работа, час	
		Лекции, час	Практические занятия, час		
ОПК-3; ИОПК3.1; ИОПК-3.2;	предприятия 3. Система управления инцидентами. Система Service Desk(«секция обслуживания»). Аудит ИБ 4. Мониторинг результатов планирования и регулирования процессов управления информационной безопасностью на основе СУИБ				Доклад/ сообщение
	Практическое занятие № 4. Построение концепции информационной безопасности предприятия		5/1		Выполнение практической работы
	Самостоятельная работа			17/31	Выполнение самостоятельной работы
	ИТОГО	**12 / 4**	**20 /4**	**49 /91**	

Примечание: *-/- объем часов соответственно для очной и очно- заочной форм обучения*

4. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

4.1. Общие методические рекомендации по освоению дисциплины, образовательные технологии

Дисциплина реализуется посредством проведения контактной работы с обучающимися(включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

При проведении учебных занятий по дисциплине обеспечивается развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплины в форме курса, составленного на основе результатов научных исследований, проводимых университетом, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

Преподавание дисциплины ведется с применением следующих видов **образовательных технологий:**

- *балльно-рейтинговая технология оценивания;*
- *электронное обучение;*
- *проблемное обучение;*
- *разбор конкретных ситуаций;*
- *информационные технологии: Miro, Google-документы, Zoom.*

Для оценки знаний, умений, навыков и уровня сформированности компетенции по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов. В основу балльно-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется в ходе текущего контроля успеваемости. Максимальное количество баллов в семестре – 100.

4.2. Методические указания для обучающихся по освоению дисциплины на занятиях лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов тематического плана. В ходе лекционных занятий раскрываются базовые вопросы в рамках каждой темы дисциплины. Обозначаются ключевые аспекты тем, а также делаются акценты на наиболее сложные и важные положения изучаемого материала.

Лекционные занятия проводятся в поточной аудитории с применением мультимедийного проектора в виде учебной презентации или в ЭИОС университета.

Отдельные темы предлагаются для самостоятельного изучения (конспектируются).

Материалы лекций являются опорной основой для подготовки обучающихся к практическим занятиям и выполнения заданий самостоятельной работы, а также к мероприятиям текущего контроля успеваемости и промежуточной аттестации по дисциплине.

4.3. Методические указания для обучающихся по освоению дисциплины на занятиях семинарского типа/ на практических занятиях

Практические (семинарские) занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы. Основной формой проведения семинаров и практических занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также решение задач и разбор примеров и ситуаций в аудиторных условиях.

Практические (семинарские) занятия обучающихся обеспечивают:

- проверку и уточнение знаний, полученных на лекциях;
- получение умений и навыков составления докладов и сообщений, обсуждения вопросов
- по учебному материалу дисциплины;

– подведение итогов занятий по рейтинговой системе, согласно технологической карте дисциплины.

Практические занятия организуются, в том числе в форме практической подготовки, которая предусматривает участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

Практическая подготовка предусматривает: выполнение практических заданий – темы 1,2,3,4.

4.4. Методические указания по самостоятельной работе обучающихся

Самостоятельная работа обеспечивает подготовку обучающегося к аудиторным занятиями мероприятиям текущего контроля и промежуточной аттестации по изучаемой дисциплине. Результаты этой подготовки проявляются в активности обучающегося на занятиях и в качестве выполненных практических заданий и других форм текущего контроля.

Самостоятельная работа студентов включает:

– изучение учебной литературы по курсу;
– подготовку докладов и выступлений по выбранной тематике;
– решение практических ситуаций и задач;
– работу с ресурсами Интернет;
– решение практических ситуаций в виде кейсов;
– подготовку к тестированию по темам курса;
– подготовку к промежуточной аттестации по курсу и др.

При выполнении заданий для самостоятельной работы рекомендуется проработка материалов лекций по каждой пройденной теме, а также изучение рекомендуемой литературы.

Для обучающихся по очно-заочной форме обучения самостоятельная работа является основным видом учебной деятельности.

Для обеспечения самостоятельной работы обучающихся используется электронный учебный курс, созданный в ЭИОС университета http://sdo.tolgas.ru/

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Вся литература, включенная в данный перечень, представлена в виде электронных ресурсов в электронной библиотеке университета (ЭБС). Литература, используемая в печатном виде, представлена в научной библиотеке университета в объеме не менее 0,25 экземпляров на одного обучающегося.

Основная литература

1. Коноплева, И. А. Управление безопасностью и безопасность бизнеса : учеб. пособие для вузов по специальности "Прикладная информатика (по обл.)" / И. А. Коноплева, И. А. Богданов. - Документ read. - Москва : ИНФРА-М, 2020. - 447 с. : табл. - (Высшее образование). - Глоссарий. - URL: https://znanium.com/read?id=354808 (дата обращения: 19.02.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-16-003230-6. - Текст : электронный.URL: https://znanium.com/read?id=354808

2. Нестеров, С. А. Основы информационной безопасности : учеб. пособие / С. А. Нестеров. - Изд. 5-е, стер. - Документ Reader. - Санкт-Петербург [и др.] : Лань, 2022. - 322 с. - (Учебники для вузов. Специальная литература). - URL: https://reader.lanbook.com/book/206279 (дата обращения: 20.10.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-8114-4067-2. - Текст : электронный. URL: https://reader.lanbook.com/book/206279

3. Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. - Изд. 4-е, стер. - Документ Reader. - Санкт-Петербург : Лань, 2022. - 124 с. - (Учебники для вузов. Специальная литература). - URL: https://reader.lanbook.com/book/217445 (дата обращения: 06.10.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-507-44201-0. - Текст : электронный.URL: https://reader.lanbook.com/book/217445

4. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учеб. пособие для студентов высш. учеб. заведений по укрупн. группе специальностей 10.05.00. "Информационная безопасность" / Ю. Н. Сычев. - Документ read. - Москва : ИНФРА-М, 2021. - 223 с. - (Высшее образование - специалитет). - Прил. - URL: https://znanium.com/read?id=364728 (дата обращения: 15.12.2022). - Режим доступа: для авториз. пользователей.-ISBN978-5-16-108817-3.-Текст: электронный. URL: https://znanium.com/read?id=364728.

Дополнительная литература

5. Бабаш, А. В. Актуальные вопросы защиты информации : монография / А. В. Бабаш, Е. К. Баранова. - Документ read. - Москва : РИОР [и др.], 2021. - 112 с. - (Научная мысль). - URL: https://znanium.com/read?id=375285 (дата обращения: 03.03.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-369-01680-0. - 978-5-16-106277-7. - Текст : электронный. URL: https://znanium.com/read?id=375285.

6. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами / А. И. Белоус, В. А. Солодуха. - Документ read. - Москва [и др.] : Инфра-Инженерия, 2020. - URL: https://znanium.com/read?id=361651 (дата обращения: 22.12.2022). - Режим доступа: для авториз. пользователей. - Текст : электронный. URL: https://znanium.com/read?id=361651

7. Дубинин, Е. А.Оценка относительного ущерба безопасности информационной системы : монография / Е. А. Дубинин, Ф. Б. Тебуева, В. В. Копытов. - Документ read. - Москва : РИОР [и др.], 2022. - 192 с. - (Научная мысль). - Прил. - URL: https://znanium.com/read?id=400262 (дата обращения: 02.03.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-369-01371-7. - 978-5-16-101863-7. - Текст : электронный.URL: https://znanium.com/read?id=400262

8. Клименко, И. С. Информационная безопасность и защита информации. Модели и методы управления : монография / И. С. Клименко. - Документ read. - Москва : Инфра-М, 2022. - 180 с. - (Научная мысль). - URL: https://znanium.com/read?id=397337 (дата обращения:

02.03.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-16-108124-2. - Текст : электронный.URL: https://znanium.com/read?id=397337

9. Конфликтно-активное управление проектами развития систем обеспечения информационной безопасности инфокоммуникационных сетей : монография / В. И. Новосельцев, С. С. Кочедыков, Д. Е. Орлова, К. А. Плющик ; под ред. В. И. Новосельцева. - Документ read. - Москва : ИНФРА-М, 2023. - 235 с. - (Научная мысль). - Прил. - URL: https://znanium.com/read?id=426480 (дата обращения: 02.03.2023). - Режим доступа: для авториз. пользователей. - ISBN 978-5-16-111199-4. - Текст : электронный. URL: https://znanium.com/read?id=426480

10. Милославская, Н. Г. Технические, организационные и кадровые аспекты управления информационной безопасностью : учеб. пособие для студентов вузов по направлению подгот. 090900 "Информ. безопасность" (уровни - бакалавр, магистр) / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - 2-е изд., испр. - Москва : Горячая линия - Телеком, 2018. - 214 с. : ил. - (Вопросы управления информационной безопасностью. Кн. 4). - Прил. - ISBN 978-5-9912-0364-7 : 377-74. - Текст : непосредственный.

11. Основы управления информационной безопасностью : учеб. пособие для вузов по направлениям подгот. (специальностям) укрупн. группы специальностей "Информ. безопасность" / А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - 2-е изд., испр. - Москва : Горячая линия -Телеком, 2016. - 244 с. : ил. - (Вопросы управления информационной безопасностью. Книга 1). - Прил. - ISBN 978-5-9912-0361-6 : 400-18. - Текст : непосредственный.

12. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учеб. пособие для вузов по направлению "Информатика и вычисл. техника" / В. Ф. Шаньгин. - Москва : ФОРУМ [и др.], 2013. - 592 с. : ил. - (Высшее образование). - Предм. указ. - ISBN 978-5-8199-0411-4. - 978-5-16-003746-2. - 118450.03.01 : 362-10. - Текст : непосредственный

5.2. Профессиональные базы данных, информационно-справочные системы, интернет-ресурсы

1. eLIBRARY.RU : научная электронная библиотека : сайт. – Москва, 2000 - . - URL: https://elibrary.ru (дата обращения: 03.12.2021). – Режим доступа: для зарегистрир. пользователей. – Текст: электронный.
2. КонсультантПлюс : справочная правовая система : сайт / ЗАО «КонсультантПлюс». – Москва, 1992 - . - URL: http://www.consultant.ru (дата обращения 03.12.2021). - Текст : электронный.
3. Электронная библиотечная система Поволжского государственного университета сервиса : сайт / ФГБОУ ВО «ПВГУС». – Тольятти, 2010 - . - URL. : http://elib.tolgas.ru(дата обращения 03.12.2021). - Режим доступа: для авториз. пользователей. - Текст : электронный.
4. Электронно-библиотечная система Znanium.com: сайт / ООО "ЗНАНИУМ". – Москва, 2011 - . - URL: https://znanium.com/ (дата обращения 03.12.2021). - Режим доступа: для авториз. пользователей. - Текст : электронный.
5. Электронно-библиотечная система Лань : сайт / ООО "ЭБС ЛАНЬ". - Москва, 2011 - . - URL: https://e.lanbook.com/ (дата обращения 03.12.2021). - Режим доступа: для авториз. пользователей. - Текст : электронный.

5.3. Программное обеспечение

Информационное обеспечение учебного процесса по дисциплине осуществляется с использованием следующего программного обеспечения (лицензионного и свободно распространяемого), в том числе отечественного производства:

№п/п	Наименование	Условия доступа
1	Microsoft Windows	из внутренней сети университета (лицензионный договор)
2	MicrosoftOffice	из внутренней сети университета (лицензионный договор)
3	КонсультантПлюс	из внутренней сети университета (лицензионный договор)
4	СДО MOODLE	из любой точки, в которой имеется доступ к сети Интернет (лицензионный договор)

6. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных учебным планом и рабочей программой дисциплины, оснащенные оборудованием и техническими средствами обучения.

Занятия лекционного типа. Учебные аудитории для занятий лекционного типа укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации (стационарные или переносные наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук), учебно-наглядные пособия (презентации по темам лекций), обеспечивающие тематические иллюстрации, соответствующие данной программе дисциплины.

Занятия семинарского типа. Учебные аудитории для занятий семинарского типа укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации (стационарные или переносные наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук).

Промежуточная аттестация. Для проведения промежуточной аттестации по дисциплине используются компьютерные классы, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета и/или учебные аудитории, укомплектованные мебелью и техническими средствами обучения.

Самостоятельная работа. Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде университета. Для организации самостоятельной работы обучающихся используются:

- компьютерные классы университета;
- библиотека (медиазал), имеющая места для обучающихся, оснащенные компьютерами с доступом к базам данных и сети «Интернет».

Электронная информационно-образовательная среда университета (ЭИОС).

Каждыйобучающийсявтечениевсегопериодаобученияобеспечениндивидуальнымнеограниченным доступом к электронной информационно-образовательной среде университета (ЭИОС) http://sdo.tolgas.ru/ из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет», как на территории университета, так и вне ее.

ЭИОС университета обеспечивает:

- доступ к учебным планам, рабочим программам дисциплин (модулей), программам практик, электронным учебным изданиям и электронным образовательным ресурсам, указанным в рабочих программах дисциплин (модулей), программах практик;
- формирование электронного портфолио обучающегося, в том числе сохранение его работ и оценок за эти работы.

В случае реализации образовательной программы с применением электронного обучения, дистанционных образовательных технологий ЭИОС дополнительно обеспечивает:

- фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения образовательной программы;
- проведение учебных занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий;
- взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействия посредством сети «Интернет».

7. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБУЧЕНИЯ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

При необходимости рабочая программа дисциплины может быть адаптирована для обеспечения образовательного процесса инвалидов и лиц с ограниченными возможностями здоровья, в том числе для дистанционного обучения. Для этого требуется заявление студента (его законного представителя) и заключение психолого-медико-педагогической комиссии (ПМПК).

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) а для инвалидов также в соответствии с индивидуальной программой реабилитации инвалида, могут предлагаться следующие варианты восприятия учебной информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

– для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифло сурдопереводчика; индивидуальные задания и консультации;

– для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации;

– для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (ФОНД ОЦЕНОЧНЫХ СРЕДСТВ) ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Для оценки знаний, умений, навыков и уровня сформированности компетенции по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов. В основу балльно-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется в ходе текущего контроля успеваемости. Максимальное количество баллов в семестре – 100.

Шкала оценки результатов освоения дисциплины, сформированности результатов обучения

Форма проведения промежуточной аттестации	Шкалы оценки уровня сформированности результатов обучения		Шкала оценки уровня освоения дисциплины		
	Уровневая шкала оценки компетенций	100 бальная шкала, %	100 бальная шкала, %	5-балльная шкала, дифференцированная оценка/балл	недифференцированная оценка
Экзамен	допороговый	ниже 61	ниже 61	«неудовлетворительно» / 2	не зачтено
	пороговый	61-85,9	61-69,9	«удовлетворительно» / 3	зачтено
			70-85,9	«хорошо» / 4	зачтено
	повышенный	86-100	86-100	«отлично» / 5	зачтено

По итогам текущей успеваемости студенту может быть выставлена оценка по промежуточной аттестации в соответствии за набранными за семестр баллами (по накопительному рейтингу).Студентам, набравшим в ходе текущего контроля успеваемости по дисциплине от 61 до 100 баллов и выполнившим все обязательные виды запланированных учебных занятий, по решению преподавателя без прохождения промежуточной аттестации выставляется оценка в соответствии со шкалой оценки результатов освоения дисциплины.

Результат обучения считается сформированным (повышенный уровень), если теоретическое содержание курса освоено полностью; при устных собеседованиях студент исчерпывающе, последовательно, четко и логически стройно излагает учебный материал; свободно справляется с задачами, вопросами и другими видами заданий, требующих применения знаний, использует в ответе дополнительный материал; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 86 до 100, что соответствует повышенному уровню сформированности результатов обучения.

Результат обучения считается сформированным (пороговый уровень), если теоретическое содержание курса освоено полностью; при устных собеседованиях студент последовательно, четко и логически стройно излагает учебный материал; справляется с задачами, вопросами и другими видами заданий, требующих применения знаний; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 61 до 85,9, что соответствует пороговому уровню сформированности результатов обучения.

Результат обучения считается несформированным, если студент при выполнении заданий не демонстрирует знаний учебного материала, допускает ошибки, неуверенно, с большими затруднениями выполняет задания, не демонстрирует необходимых умений, качество выполненных заданий не соответствует установленным требованиям, качество их выполнения оценено числом баллов ниже 61, что соответствует допороговому уровню.

Формы текущего контроля успеваемости

Формы текущего контроля	Количество контрольных точек	Количество баллов за 1 контр. точку	Макс. возм. кол-во баллов
Доклад/сообщение	3	10	30
Решение практических заданий	4	15	60
Творческий рейтинг (участие в конференциях, олимпиадах). Дополнительные баллы за активное изучение дисциплины	1	10	10
			100 баллов

Система оценивания представлена в электронном учебном курсе по дисциплине http://sdo.tolgas.ru/.

8.2. Типовые контрольные задания или иные материалы для ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

8.2.1. Типовые задания к практическим (семинарским) занятиям (темы докладов/сообщений)

Практическое занятие № 1. Изучение нормативной базы документов в области ИБ

Вопросы для обсуждения

1. Лицензирование (ФЗ РФ от 08.08.2001 № 128-ФЗ).
2. Техническое регулирование (ФЗ РФ от 27.12.2002 № 184-ФЗ).
3. Стандарт (ФЗ РФ от 27.12.2002 № 184-ФЗ).
4. Сертификация (ФЗ РФ от 27.12.2002 № 184-ФЗ).
5. Нормативно-правовая база управления ИБ (ISO/IEC 17799:2005 и ISO/IEC 27001:2005).
6. Стадии реализации системы управления информационной безопасностью: 1) формирование политики в области рисков анализ бизнес-процессов; 3) анализ рисков; 4) формирование целевой концепции.

Практическое занятие № 2. Изучение методики оценки рисков информационной безопасности

Вопросы для обсуждения

1. Что понимается под информационной безопасностью (ИБ)?
2. Каковы ее основные составляющие?
3. На какие виды классифицируют информацию?
4. Как различается информация по правовому режиму доступа?
5. Какую роль могут играть общедоступная и ограниченного доступа информации в организации?
6. Что составляет информацию ограниченного доступа?
7. Кратко охарактеризуйте различные виды секретной и конфиденциальной информации.
8. Что представляет собой система управления информационной безопасностью (СУИБ)? Каковы ее цели и задачи?
9. Какие вы знаете четыре стадии реализации системы управления информационной безопасностью? Кратко охарактеризуйте их.
10. Перечислите и кратко поясните основные этапы разработки и внедрения политики безопасности.
11. Назовите основные принципы политики безопасности.
12. Какие меры безопасности способствуют правильному обеспечению и поддержке политики информационной безопасности на предприятии?

13. Какие методы регулирования используются в области информационной безопасности со стороны государства?
14. Что представляет собой нормативно-правовая база управления ИБ?
15. Какие документы определяют ответственность субъектов за нарушения в сфере ИБ?

Задание

1. Загрузите ГОСТ Р ИСО/МЭК 27005—2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности»
2. Ознакомьтесь с Приложениями C, D и E ГОСТа.
3. Выберите три различных информационных актива организации (см. вариант).
4. Из Приложения D ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.
5. Пользуясь Приложением C ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.
6. Пользуясь одним из методов (см. вариант) предложенных в Приложении E ГОСТа произведите оценку рисков информационной безопасности.
7. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

Содержание отчета

1. Титульный лист
2. Содержание
3. Задание
4. Обоснование выбора информационных активов организации
5. Оценка ценности информационных активов
6. Уязвимости системы защиты информации
7. Угрозы ИБ
8. Оценка рисков
9. Выводы

Перечень докладов по теме 1 «Основные понятия науки об управлении. Системный, процессный, нормативный подходы»

1. Школа научного управления. Ф.У. Тейлор, Г.Форд.
2. Инновации как объект управления.
3. Кибернетический подход в управлении.
4. Синергетический подход в управлении.
5. Принципы и подходы проектного менеджмента.
6. Бизнес-процесс как объект управления.
7. Информационные технологии в управленческой деятельности.
8. Ситуационное управление.
9. Понятие организационной структуры.
10. Управление рисками.
11. Оценка эффективности системы управления.
12. Делегирование полномочий Функции управления
13. 34. Теория рефлексивного управления
14. Методы коллективного принятия решений.
15. Системы менеджмента качеством.
16. Управление изменениями: принципы и подходы
17. Управление знаниями.
18. Гибкие технологии управления.
19. Модели управления изменениями.
20. Принятия решений в условиях неопределенности.
21. Функциональный и процессный подход в управлении.

22. Направления развития современной теории и практики управления.
23. Концепция сбалансированных показателей (BalancedScorecard).

Практическое занятие № 3. Построение функциональной модели процессов обеспечения информационной безопасности с помощью графических нотаций и в соответствии с требованиями ТЗ.

Цель работы: Построение функциональной IDEF0 -модели СЗИ и ее анализ.

Задание. Построить трехуровневую IDEF0-модель СЗИ и формализовать требования к ней.

Ход работы

1. Запустите Process Modeler.
2. Создайте новую модель, нажав на кнопку New Model. Внесите имя модели «Функциональная модель СЗИ» и выберите Type - IDEF0 (рис.2.1).

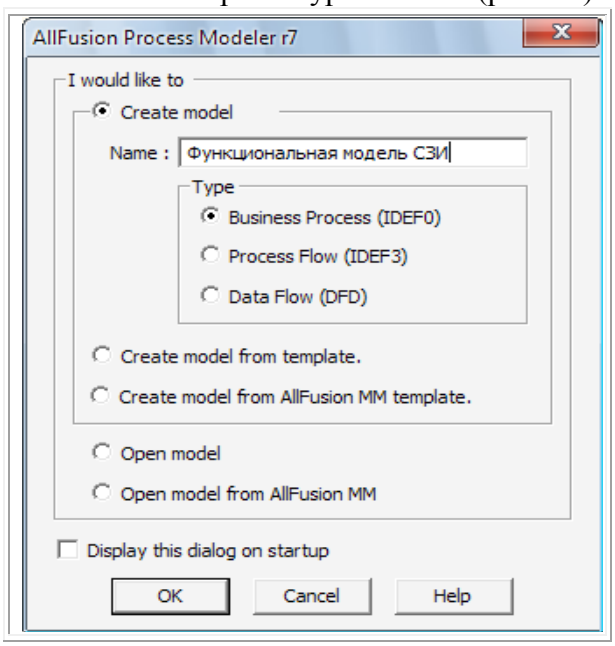


Рис. 2.1. Создание новой модели

3. Появляется диалог «Properties for New Models», в котором можно выставить значения основных свойств новой модели.
4. Автоматически создается контекстная диаграмма.
5. Закладки в Model Explorer (окно слева) позволяют переходить от одного режима просмотра модели к другому и предоставляют возможность быстро переходить от одной диаграммы к другой.
7. Если Вам непонятно как выполнить то или иное действие, Вы можете вызвать помощь - клавиша F1 или меню Help.
8. Перейдите в меню Model/Model Properties. В закладке General диалога Model Properties следует внести имя проекта «Функциональная модель СЗИ», имя автора и тип модели - Time Frame {AS-IS}.
9. В полях закладки «Purpose» внесите Цель - «Цель: Определение и распределение функций для управления СЗИ» и Точку зрения - «Точка зрения: Директор».
10. В поля закладки «Definition» внесите определение «Учебная модель, описывающая функциональную область СЗИ» и «Scope» - «Общие функции СЗИ, характерные для любой хозяйственной деятельности».
11. В закладке Source - «Материалы курса по работе с AllFusion Process Modeler».
12. Перейдите в меню Diagram/Diagram Properties и установите свойства диаграммы.

13. Перейдите на контекстную диаграмму и правой кнопкой мыши щелкните по работе. В контекстном меню выберите Name. В закладке Name внесите имя «Обеспечить защиту информации».

14. В закладке Definition внесите определение «Текущее состояние СЗИ».

15. В закладке Status установите WORKING.

16. Создайте интерфейсные дуги на контекстной диаграмме, как показано в табл.2.1.

Таблица 2.1

Arrow Name	Arrow Definition	Arrow Type
Персонал		Mechanism
Средства СЗИ	Программные и технические средства СЗИ	Mechanism
Администратор СЗИ	Орган управления СЗИ	Mechanism
Угрозы безопасности	Все возможные угрозы	Input
Политика безопасности	Комплекс превентивных мер по защите конфиденциальной безопасности	Control
Нормативы	Действующие законодательные и правовые акты	Control
Совокупный риск	Суммарные негативные последствия от реализации угроз	Output

В результате должна получиться диаграмма, показанная на рис.2.2.

17. Декомпозируйте основную функцию, показанную на рис.2.2. В результате должна получиться диаграмма, изображенная на рис.2.3. Как видно из рис. 2.3, функцию «Обеспечить защиту информации» составляют функции:

· Управлять доступом;

· Вести регистрацию и учет;

· Шифровать данные;

· Обеспечить целостность.

Для изменения свойств работ после их внесения в диаграмму можно воспользоваться словарем объектов модели. Вызов словаря - Model/Diagram Object Editor... или Dictionary/Activity...

Описав имя и свойства работы в словаре, ее можно будет внести в диаграмму позже с помощью кнопки в палитре инструментов. При этом нельзя удалять работу из словаря, если она используется на какой-либо диаграмме. Если удалить работу из диаграммы, из словаря она не удаляется. Имя и описание такой работы может быть использовано в дальнейшем. Для добавления работы в словарь (Dictionary / Activity) щелкните на пустой строке, внесите имя и свойства работы. Для удаления всех имен работ, не использующихся в модели, щелкните по Purge.

18. Декомпозируйте функции диаграммы А0 (рис.2.3), как показано на рис. 2.4 – 2.7

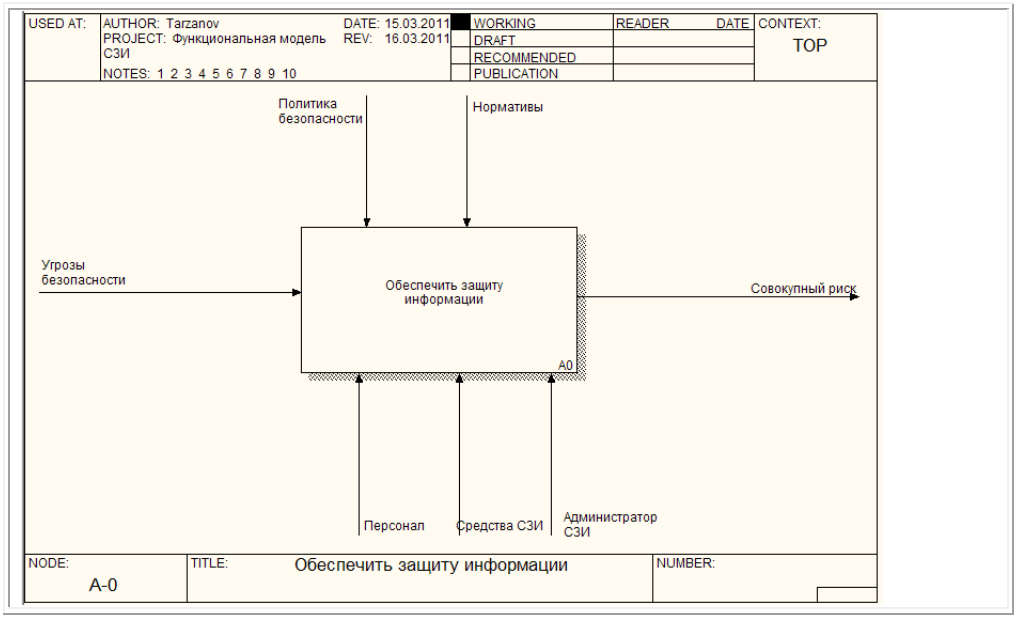


Рис. 2.2. Контекстная диаграмма модели

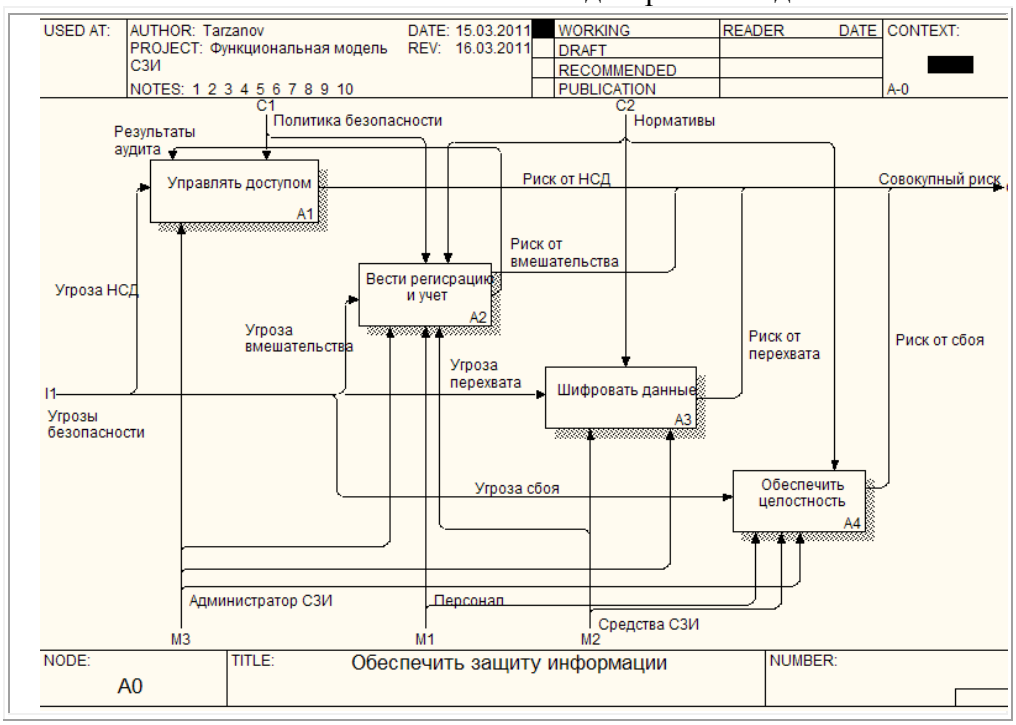


Рис. 2.3. Декомпозиция основной функции

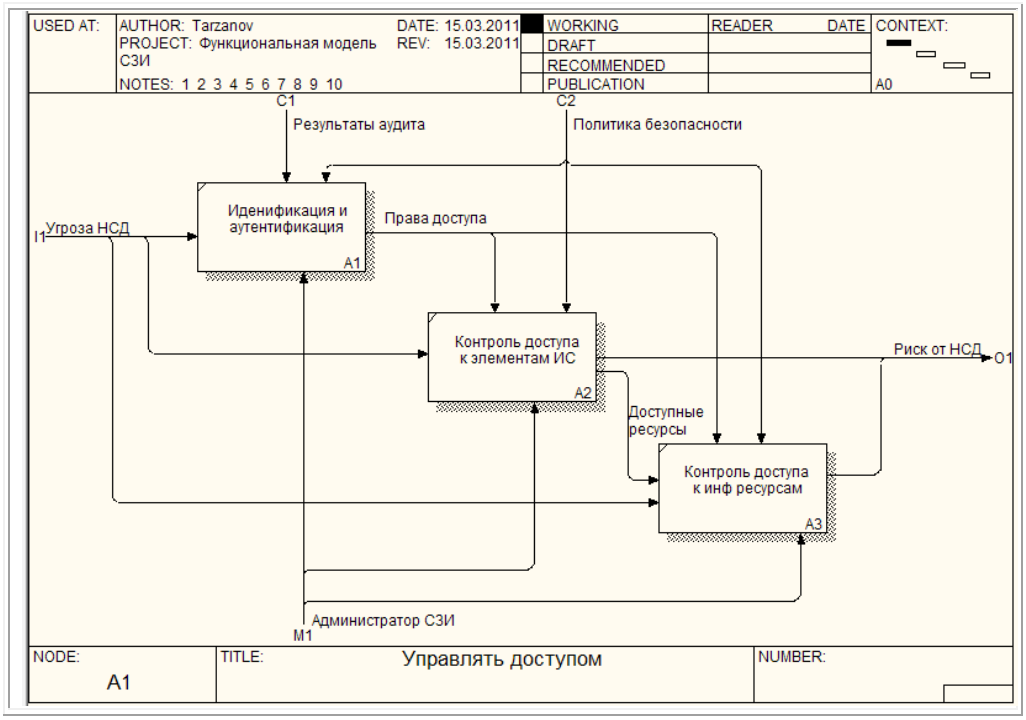


Рис. 2.4. Декомпозиция функции «Управлять доступом»

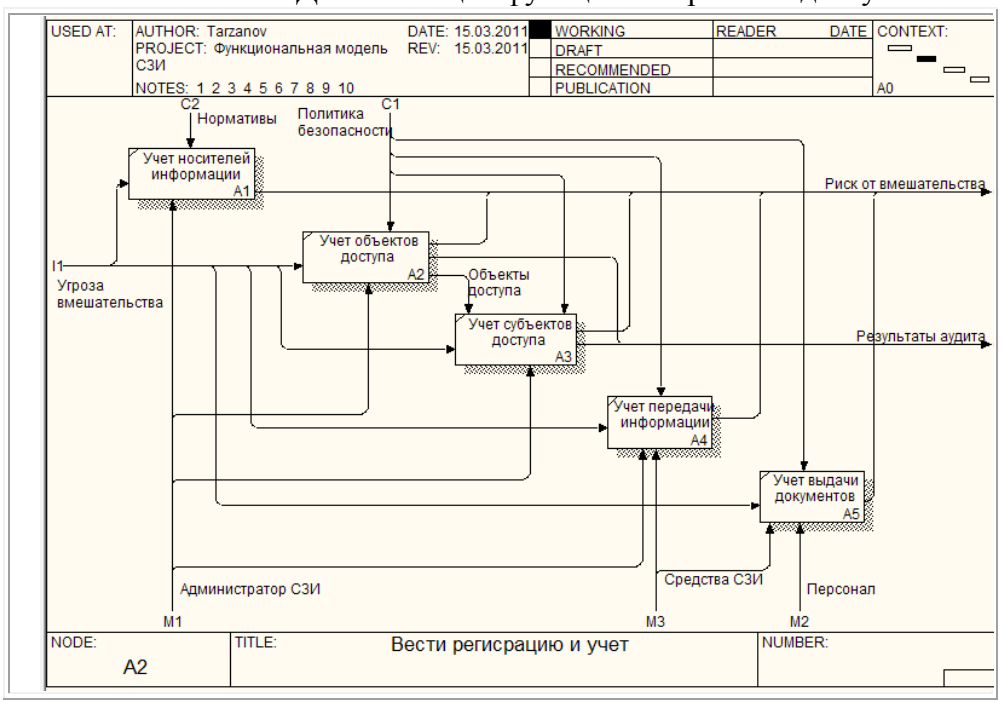


Рис. 2.5. Декомпозиция функции «Вести регистрацию и учет»

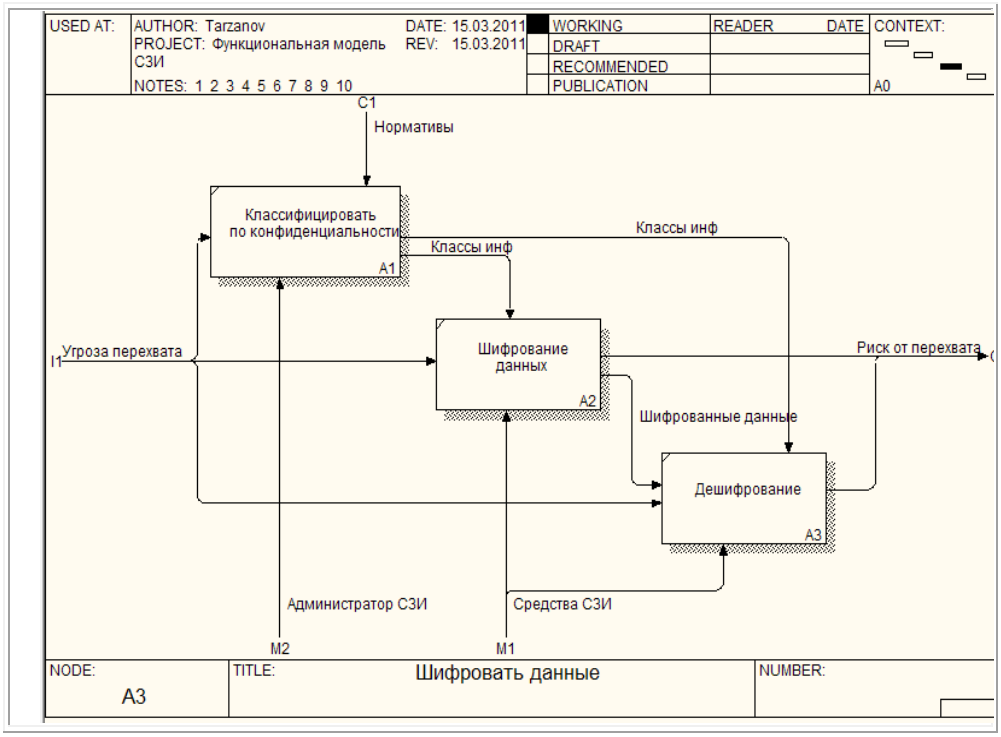


Рис. 2.6. Декомпозиция функции «Шифровать данные»

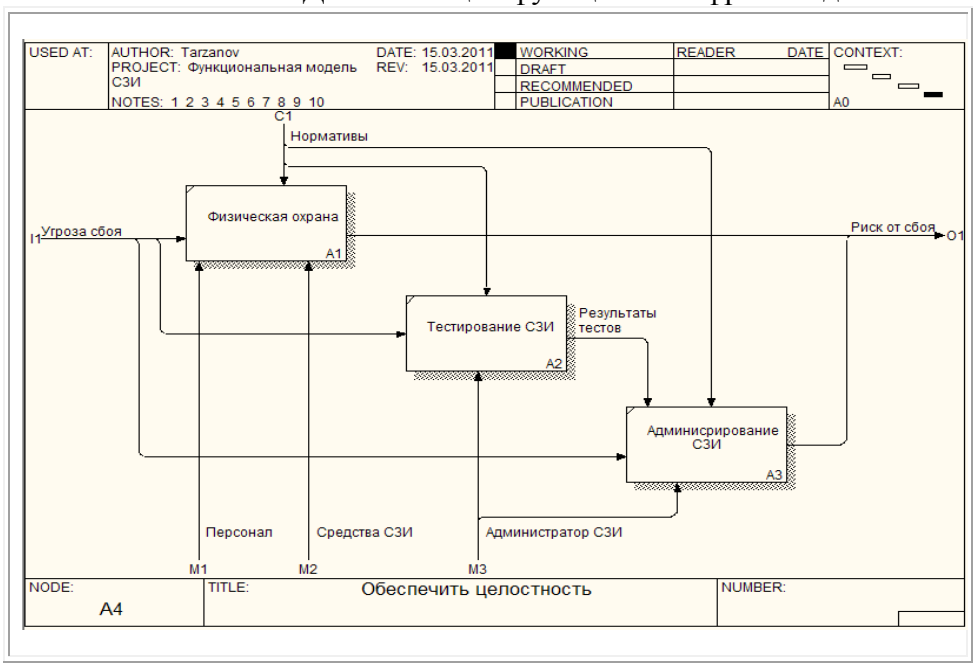


Рис. 2.7. Декомпозиция функции «Обеспечить целостность»

19. Перейдите на диаграмму A0. В свойствах работ на вкладе Definition по табл. 2.2 заполните требования, которые должны быть реализованы данной функцией для класса защищенности 1А.

Таблица 2.2- Формализованные требования к защите информации от НСД для АС первой группы

Подсистемы и требования	Классы				
1Д	1Г	1В	1Б	1А	
1. Подсистема управления доступом 20.6. Идентификация, проверка подлинности и контроль доступа субъектов: • в систему • к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ • к программам • к томам, каталогам, файлам, записям, полям записей 1.2. Управление потоками информации	+ - - - -	+ + + + + -	+ + + + +	+ + + + +	+ + + + +
2. Подсистема регистрации и учета 2.1. Регистрация и учет: • входа (выхода) субъектов доступа в (из) систему (узел сети) • выдачи печатных (графических) выходных документов • запуска (завершения) программ и	+ - - - - - - - + - -	+ + + + + -	+ + + + +	+ + + + +	+ + + +

процессов (заданий, задач) • доступа программ субъектов доступа, защищаемым файлам, включая их создание, удаление, передачу по линиям и каналам связи • доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, программам, томам, каталогам, файлам, записям, полям записей • изменения полномочий субъектов доступа • создаваемых защищаемых объектов доступа 2.2. Учет носителей информации 2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей 2.4. Сигнализация попыток нарушения защиты		- + + -	+ + + +	+ + + +	+ + + + + +
3. Криптографическая подсистема 3.1. Шифрование конфиденциальной информации 3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах 3.3. Использование аттестованных (сертифицированных) криптографических средств	- - -	- - -	- - -	+ - +	+ + +
4. Подсистема обеспечения целостности 4.1. Обеспечение целостности программных средств и обрабатываемой информации 4.2. Физическая охрана средств вычислительной техники и носителей информации 4.3. Наличие администратора (службы) защиты информации в АС 4.4. Периодическое тестирование СЗИ НСД 4.5. Наличие средств восстановления СЗИ НСД 4.6. Использование сертифицированных средств защиты	+ + - + + -	+ + - + + -	+ + + + + +	+ + + + + +	+ + + + + +

20. Сгенерируйте отчет по этой диаграмме (Tools / Reports / Diagram Object Report), настроив параметры отчета, как показано на рис.2.8.

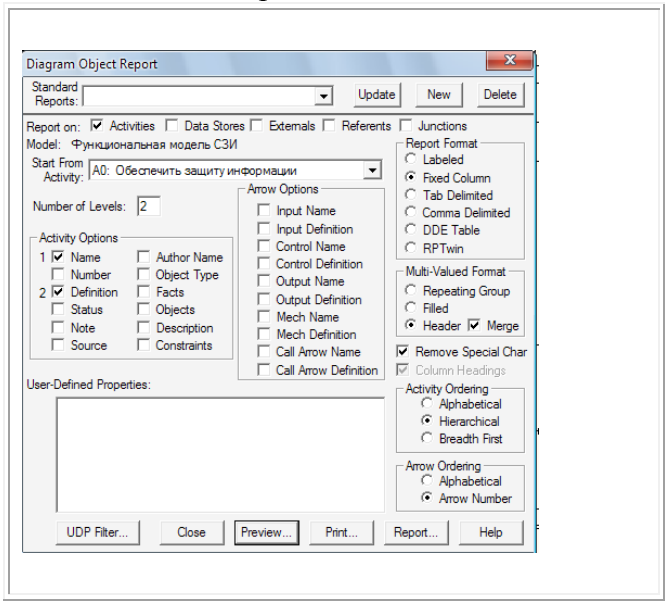
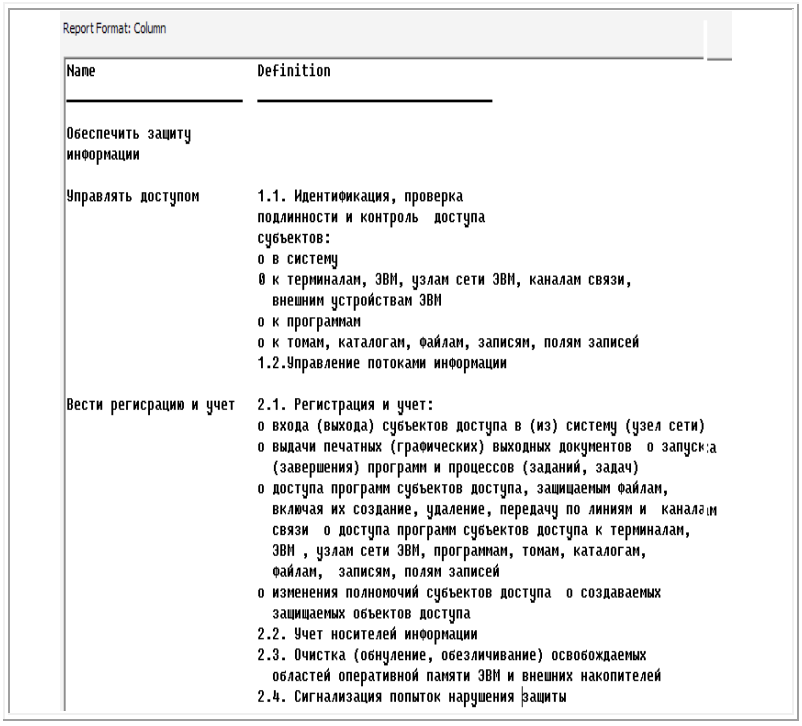


Рис. 2.8. Настройка параметров отчета о требованиях

Результаты отчета можно увидеть, нажав кнопку Preview (рис.2.9).


Report Format: Column

Name	Definition
Обеспечить защиту информации	
Управлять доступом	1.1. Идентификация, проверка подлинности и контроль доступа субъектов: о в систему 0 к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ о к программам о к томам, каталогам, файлам, записям, полям записей 1.2.Управление потоками информации
Вести регисрацию и учет	2.1. Регистрация и учет: о входа (выхода) субъектов доступа в (из) систему (узел сети) о выдачи печатных (графических) выходных документов о запуска (завершения) программ и процессов (заданий, задач) о доступа программ субъектов доступа, защищаемым файлам, включая их создание, удаление, передачу по линиям и каналам связи о доступа программ субъектов доступа к терминалам, ЭВМ , узлам сети ЭВМ, программам, томам, каталогам, файлам, записям, полям записей о изменения полномочий субъектов доступа о создаваемых защищаемых объектов доступа 2.2. Учет носителей информации 2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей 2.4. Сигнализация попыток нарушения защиты

Рис. 2.9. Отчет о требованиях к СЗИ (фрагмент)

21. Сгенерируйте отчет о распределении обязанностей по функциям СЗИ. Для этого настройте параметры отчета, как показано на рис.2.10.

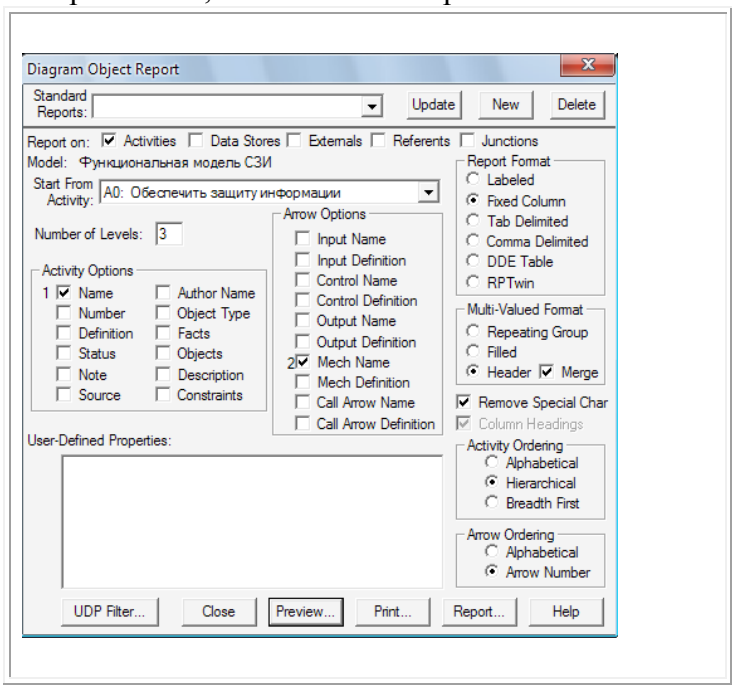


Рис. 2.10. Настройка параметров отчета о распределении обязанностей

Результаты отчета показаны на рис.2.11.

Report Format: Column

Name	Mechanism Name
Обеспечить защиту информации	Персонал
	Средства СЗИ
	Администратор СЗИ
Управлять доступом	Администратор СЗИ
Иденификация и аутентификация	Администратор СЗИ
Контроль доступа к элементам ИС	Администратор СЗИ
Контроль доступа к инф ресурсам	Администратор СЗИ
Вести регисрацию и учет	Администратор СЗИ
	Персонал
	Средства СЗИ
Учет носителей информации	Администратор СЗИ

Рис. 2.11. Отчет о распределении обязанностей (фрагмент)

Вероятность подбора разрешенной комбинации за время t_{max} составит:

$$P_н^t = \begin{cases} 1, & \text{при } \frac{t_{max}}{t_{он}K} \geq 1; \\ \frac{t_{max}}{t_{он}K}, & \text{в противном случае.} \end{cases} \qquad (3.1)$$

В уравнении (1.1) параметр К определяется из выражений: $\sum_{i=1}^{K} \frac{1}{N-N_i} \geq 1$ – для случая одной разрешенной комбинации, (3.2)

где $\frac{1}{N-N_i} = p_i$ – вероятность подбора разрешенной комбинации на i – й попытке;

N_i – число использованных комбинаций к моменту i – й попытки;

$K = \frac{N+1}{\chi+1}$ – для случая χ разрешенных комбинаций. (3.3)

Пусть N=10, t_{max}=8 час, $t_{он}$=0,01 час, χ=1.

Тогда

$$p_\Sigma = \frac{1}{10-1} + \frac{1}{10-2} + \ldots + \frac{1}{10-6} \approx 0{,}995 \quad \text{K=6.}$$

Следовательно, подставив исходные и полученные данные в (3.1) вероятность НСД составит $p_н^t$=1.

Следует обратить внимание на параметр N. Например, если N=10, то это значит, что существует всего 10 возможных комбинаций (масок) пароля, а другие комбинации использовать просто невозможно.

Если же в пароле использовать 10 цифр, а сам пароль длиной 8 символов, то $N=10^8$. Следовательно,

$K \approx \frac{10^8}{10} = 10^7$.

Тогда $p_н^t = \frac{8}{10^{-2}10^7} = 8 \cdot 10^{-5}$.

Однако, если злоумышленником являются специальное программное средство, то $t_{он}$ @ 10^{-6} … 10^{-7}. С учетом этого $p_н^t$@ 1.

Вероятность подбора разрешенной комбинации за время t_{max} составит:

$$p_{н}^{t} = \begin{cases} \frac{N_в}{К}, & \text{при } \frac{t_{max}}{t_{он}К} \geq 1; \\ \frac{t_{max}N_в}{t_{он}К^2}, & \text{в противном случае.} \end{cases} \quad (3.4)$$

Реализуем приведенные аналитические модели средствами MS Office Excel.

1. На новом листе MS Office Excel создайте таблицу, как показано на рис.3.1.

	A	B
1		
2		
3		
4	**Параметр парольной системы**	**Значе**
5	Общее число возможных комбинаций пароля (N)	
6	Число разрешенных комбинаций пароля ($\chi > 1$)	
7	Максимальное время действий злоумышленника (tmax, мин)	
8	Среднее время набора одной комбинации пароля (tон, мин)	
9	Среднее число попыток до подбора разрешенной комбина-ции (К)	
10	Число набора до срабатывания ограничителя (Nв)	

Рис. 3.1. Параметры парольной системы

При этом для ячейки B9 введите формулу =(B5+1)/(B6+1) (предполагая, что существует более одной разрешенной комбинации пароля).

2. Рассчитайте показатели эффективности парольной системы (рис.3.2). При этом для ячейки B14 используйте логическую функцию ЕСЛИ (рис.3.3), а для ячейки B18 – рис.3.4.

13	1. Парольная система без ограничителя	
14	**Вероятность подбора разрешенной комбинации**	**1.**
15		
16		
17	2. Парольная система с ограничителем	
18	**Вероятность подбора разрешенной комбинации**	**0.03**

Рис. 3.2. Оценка эффективности парольной системы

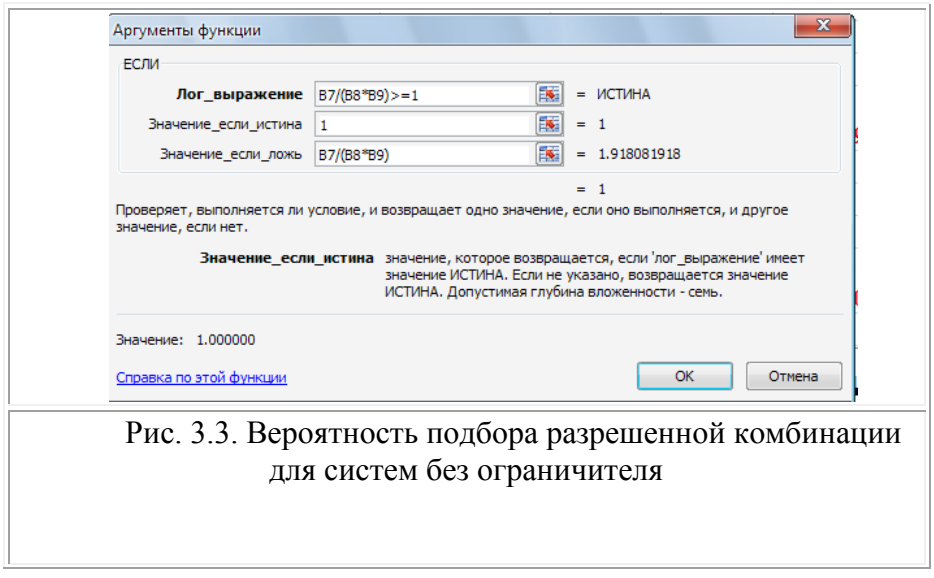


Рис. 3.3. Вероятность подбора разрешенной комбинации для систем без ограничителя

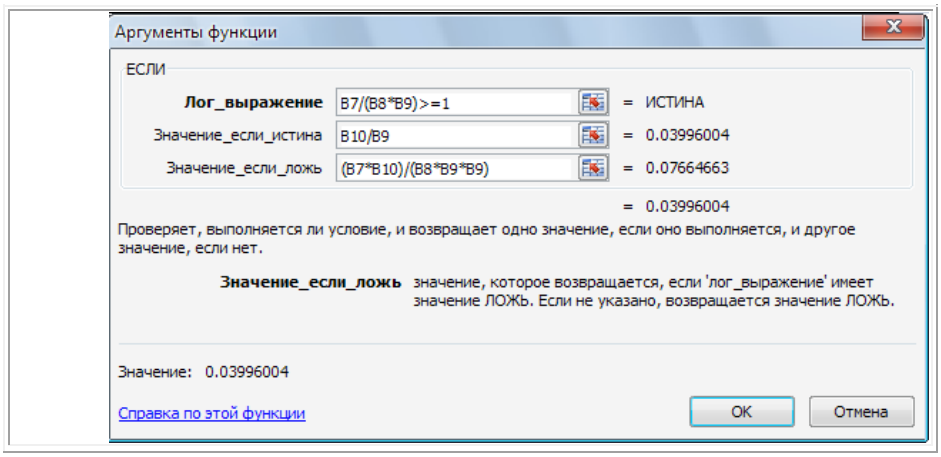


Рис. 3.4. Вероятность подбора разрешенной комбинации для систем с ограничителем

3. Постройте сравнительную диаграмму полученных результатов (рис.3.5).

Рис. 3.5. Эффективность парольных систем

4. Изменяя общее число возможных комбинаций пароля (N) оцените изменение вероятности подбора разрешенной комбинации (рия.3.6).

	Параметр парольной системы	Значение		
5	Общее число возможных комбинаций пароля (N)	1000	10000	100000
6	Число разрешенных комбинаций пароля ($\chi > 1$)	3	3	3
7	Максимальное время действий злоумышленника (tmax, мин)	480	480	480
8	Среднее время набора одной комбинации пароля (tон, мин)	1	1	1
9	Среднее число попыток до подбора разрешенной комбина-ции (К)	250.250	2500.250	25000.250
10	Число набора до срабатывания ограничителя (Nв)	10	10	10
11				
12				
13	1. Парольная система без ограничителя			
14	**Вероятность подбора разрешенной комбинации**	**1.000000**	**0.191981**	**0.019200**
15				
16				
17	2. Парольная система с ограничителем			
18	**Вероятность подбора разрешенной комбинации**	**0.03996004**	**0.000768**	**0.000008**

Рис. 3.6. Изменение вероятности подбора в зависимости от числа возможных комбинаций

5. Постройте график изменения вероятности подбора (рис.3.7).

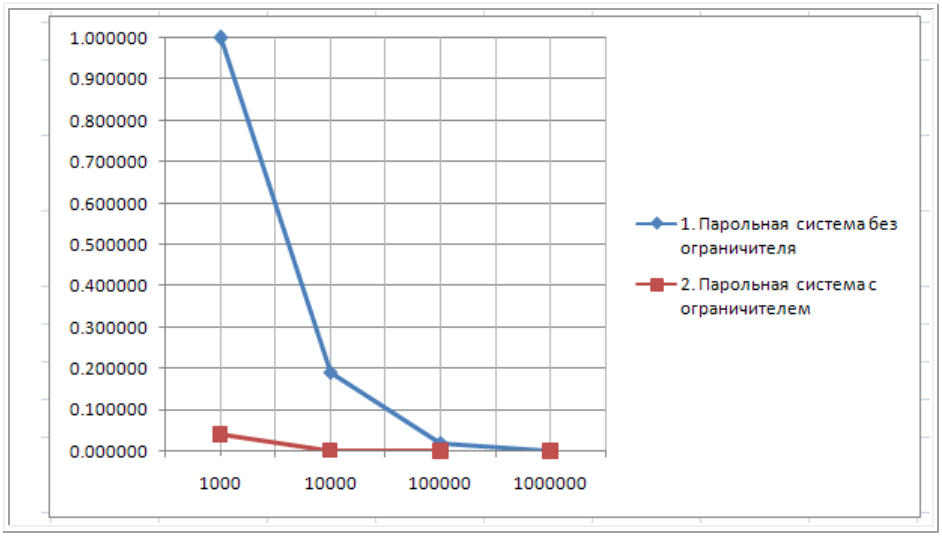


Рис. 3.7. График изменения вероятности подбора в зависимости от числа возможных комбинаций

6. Определите, каким должно быть среднее время набора одной комбинации пароля, чтобы вероятность подбора (для системы без ограничителя) была не менее 0,85. Для этого необходимо воспользоваться надстройкой MS Office Excel Поиск решения (пункт меню Данные / Поиск решения). Если данная надстройка недоступна, необходимо ее активировать выбрав Кнопка Office / Параметры Excel / Надстройки. На открывшейся вкладке нажать на кнопку Перейти и выбрать Поиск решения. Выбрать пункт меню Данные / Поиск решения. В диалоговом окне заполнить параметры, как показано на рис.3.8 и найти оптимальное решение.

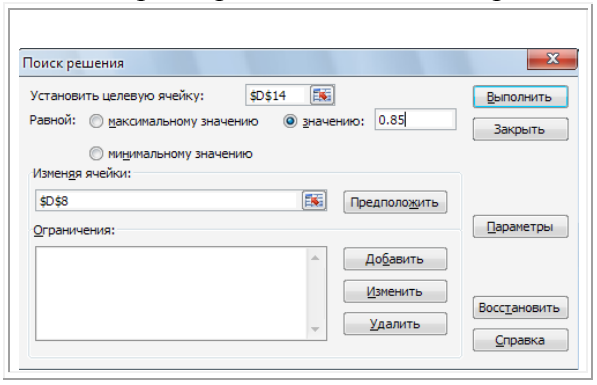


Рис. 3.8. Настройка параметров поиска решения

Перечень докладов по теме 2 «Проектирование системы управления информационной безопасностью на предприятии»

1. Формирование матрицы и модели доступа к управлению информационной безопасностью.
2. Основные виды угроз информационной безопасности.
3. Модель нарушителя информационной безопасности.
4. Мероприятия по управлению информационной безопасностью на предприятии. Определение режима управления информацией на предприятии.
5. Разработка подсистемы управления доступом защищаемой информации.
6. Контроль за работой средствами управления информационной безопасности (СУИБ) на предприятии.
7. Мониторинг и оценка рисков управления информационной безопасностью.

Практическое занятие № 4. Построение концепции информационной безопасности предприятия

Цель работы: знакомство с основными принципами построения концепции ИБ предприятия, с учетом особенностей его информационной инфраструктуры.

Задание. Используя предложенные образцы, разработать концепцию информационной безопасности компании (см. вариант), содержащую следующие основные пункты (приведен примерный план, в который в случае необходимости могут быть внесены изменения):

1. Общие положения
1.1. Назначение Концепции по обеспечению информационной безопасности.
1.2. Цели системы информационной безопасности
1.3. Задачи системы информационной безопасности.
2. Проблемная ситуация в сфере информационной безопасности
2.1. Объекты информационной безопасности.
2.2. Определение вероятного нарушителя.
2.3. Описание особенностей (профиля) каждой из групп вероятных нарушителей.
2.4. Основные виды угроз информационной безопасности Предприятия.
Классификации угроз.
Основные непреднамеренные искусственные угрозы.
Основные преднамеренные искусственные угрозы.
Общестатистическая информация по искусственным нарушениям информационной безопасности.
Оценка потенциального ущерба от реализации угрозы.
3. Механизмы обеспечения информационной безопасности Предприятия
3.1. Принципы, условия и требования к организации и функционированию системы информационной безопасности.
3.2. Основные направления политики в сфере информационной безопасности.
3.3. Планирование мероприятий по обеспечению информационной безопасности Предприятия.
3.4. Критерии и показатели информационной безопасности Предприятия.
4. Мероприятия по реализации мер информационной безопасности Предприятия
4.1. Организационное обеспечение информационной безопасности.
Задачи организационного обеспечения информационной безопасности.
Подразделения, занятые в обеспечении информационной безопасности.
Взаимодействие подразделений, занятых в обеспечении информационной безопасности.
4.2. Техническое обеспечение информационной безопасности Предприятия.
Общие положения.
Защита информационных ресурсов от несанкционированного доступа.
Средства комплексной защиты от потенциальных угроз.
Обеспечение качества в системе безопасности.
Принципы организации работ обслуживающего персонала.
4.3. Правовое обеспечение информационной безопасности Предприятия.
Правовое обеспечение юридических отношений с работниками Предприятия.
Правовое обеспечение юридических отношений с партнерами Предприятия.
Правовое обеспечение применения электронной цифровой подписи.
4.4. Оценивание эффективности системы информационной безопасности Предприятия.
5. Программа создания системы информационной безопасности Предприятия

Содержание отчета

1. Титульный лист
2. Содержание
3. Задание
4. Концепция ИБ заданного предприятия по плану, приведенному в задании

Перечень докладов по теме 3 «Оценка рисков информационной безопасности на предприятии»

1. Способы оценки информационной безопасности.
2. Процесс оценки информационной безопасности.
3. Основные элементы процесса оценки.
4. Контекст оценки информационной безопасности организации.
5. Мероприятия и выходные данные процесса оценки.
6. Сбор свидетельств оценки и проверка их достоверности.
7. Измерение и оценивание атрибутов объекта оценки.
8. Способы измерения атрибутов объекта оценки.
9. Применение типовых моделей оценки на основе оценки процессов и уровней зрелости. процессов для оценки информационной безопасности.
10. Модель оценки информационной безопасности на основе оценки процессов.
11. Оценка информационной безопасности на основе модели зрелости процессов.
12. Риск-ориентированная оценка информационной безопасности.

8.3. Типовые контрольные задания или иные материалы для проведения ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Форма проведения промежуточной аттестации по дисциплине: экзамен (по результатам накопительного рейтинга или в форме компьютерного тестирования).

Устно-письменная форма по вопросам к экзамену предполагается, как правило, для сдачи академической задолженности.

Перечень вопросов для подготовки к экзамену

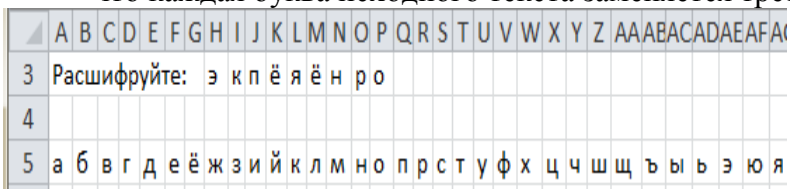
УК-3. ИУК-3.2: Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели

1. Какой документ регламентирует обеспечение правовых условий использования электронной цифровой подписи в электронных документах?
2. Что является основным документом, обеспечивающим защиту персональных данных?
3. Под какую статью УК РФ попадает такое киберпреступление, как неправомерный доступ к компьютерной информации?
4. Дайте определение понятия «Критерий экономической безопасности - это»
5. Какой государственный стандарт содержит «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер»?
6. Дайте определение информационной безопасности.
7. В виде совокупности каких уровней можно представить организационную структуру системы обеспечения информационной безопасности АС организации?
8. Дайте определение понятия «Система защиты информации (СЗИ)»
9. Дайте определение понятия «Профессиональная тайна»
10. В чём разница между служебными и коммерческими секретами?
11. Дайте определение понятия «Персональные данные»
12. Какими факторами могут быть обусловлены информационные угрозы?
13. Запишите виды информационных угроз для государства
14. Запишите виды информационных угроз для компании.
15. Запишите виды информационных угроз для личности (физического лица).
16. Дайте определение Макровируса
17. Дайте определение экономической безопасности

18. Какой документ устанавливает классификацию и перечень факторов, воздействующих на безопасность защищаемой информации, в целях обоснования угроз безопасности информации и требований по защите информации на объекте информатизации
19. Какой орган впервые определил критерии установления коммерческого мошенничества.
20. Закончите определение. Согласно Стратегии экономической безопасности РФ до 2030 года угрозы экономической безопасности – это…

ОПК-1. ИОПК-1.1-ИОПК-1.2: Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание

1. Перечислите функции, выполняемые антивирусом Касперского.
2. Дайте краткую характеристику антивирусам сканерам
3. Дайте краткую характеристику антивирусам мониторам
4. Запишите меры профилактики заражения ПК вирусом.
5. Запишите основные пути проникновения вирусов на компьютер
6. Перечислите вредные действия вирусов.
7. Дайте определение понятия «Персональные данные»
8. Какими факторами могут быть обусловлены информационные угрозы?
9. Запишите виды информационных угроз для государства
10. Запишите виды информационных угроз для компании
11. Запишите виды информационных угроз для личности (физического лица)
12. Дайте определение Макровируса
13. Макровирусы заражают файлы – документы и электронные таблицы офисных приложений. Для анализа макровирусов необходимо получить текст их макросов. При помощи, каких команд можно это сделать для нешифрованных (не-стелс) файлов?
14. Если на компьютере нет антивирусных программ, то каким образом можно восстановить документы Word и Excel заражённых вирусом?
15. Запишите последовательность действий, которые необходимо выполнить для того, чтобы восстановить пораженные документы Word и Excel в случае того, если на компьютере нет антивирусных программ
16. Запишите, какие действия необходимо выполнить, для защиты файлов от макровирусов, если на компьютере нет антивирусных программ.
17. Запишите виды информационных угроз для государства.
18. Какие действия необходимо выполнить в MS Office чтобы зашифровать файл и задать пароль для его открытия?
19. Запишите алгоритм процесса создания архива с паролем в WinRAR. и архив будет создан с паролем.
20. Расшифруйте слово «экпёяёнро», закодированное с помощью шифра Цезаря. Известно, что каждая буква исходного текста заменяется третьей после нее буквой.



ОПК-3. ИОПК-3.1-ИОПК-3.2: Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности.

1. Какие особенности проектирования и разработки организационно-распорядительных документов по обеспечению ИБ регламентированы ГОСТ Р ИСО /МЭК 27005-2010
2. Соотнести между собой процессы системы менеджмента информационной безопасности и процесса менеджмента риска информационной безопасности

3. Что должно быть реализовано в организации при управлении контентом. В соответствии с требованиями ГОСТ Р ИСО/МЭК 27005-2010
4. Перечислить в качестве примера цели менеджмента риска информационной безопасности, которые могут быть указаны в документе «Руководство по реализации» (ГОСТ Р ИСО/МЭК 27005-2010)
5. С учетом чего рекомендовано в организации формировать критерии оценки рисков ИБ?
6. Что такое идентификация риска и какова цель идентификации
7. Роль организационной структуры менеджмента риска информационной безопасности
8. Общее описание оценки риска ИБ
9. Как происходит определение активов организации для их защиты от рисков?
10. Привести пример того, в каких областях деятельности организации могут быть выявлены уязвимости
11. Привести пример последствий, которые могут быть вызваны потерей конфиденциальности, целостности и доступности
12. Привести пример, на основе чего организации могут определять операционные последствия выявленного сценария компьютерного инцидента?
13. В чем заключается управление информационной безопасностью в организации
14. Чем занимается отдел информационной безопасности в организации и что входит в его основные задачи?
15. Каково назначение процесса управления информационной безопасностью организации с точки зрения процессного подхода?
16. Назовите предпосылки разработки политики безопасности предприятия