МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Астраханский государственный университет имени В. Н. Татищева»
(Астраханский государственный университет им. В. Н. Татищева)

СОГЛАСОВАНО
Руководитель ОПОП

Р.Ю. Демина

«04» апреля 2024 г.

УТВЕРЖДАЮ
И.о. заведующего кафедрой
информационной безопасности

Т.Г. Гурская

«04» апреля 2024 г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

## Проектирование и эксплуатация защищенных информационных систем

| | |
|---|---|
| Составитель(-и) | **Шукралиева Д.Э. доцент кафедры информационной безопасности; Корякова В.А., ассистент кафедры информационных технологий, начальник отдела информационной безопасности** |
| Согласовано с работодателями | **Давидюк Н.В., доцент, кандидат технических наук, заведующий кафедрой «Информационная безопасность» ФГБОУ ВО «Астраханский государственный технический университет; Барсуков В.А., начальник отдела информационной безопасности Управления корпоративной защиты ООО «Газпром добыча Астрахань»** |
| Направление подготовки | **10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ** |
| Направленность (профиль) ОПОП | **ОРГАНИЗАЦИЯ И ТЕХНОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ** |
| Квалификация (степень) | **бакалавр** |
| Форма обучения | **Очная** |
| Год приема | **2023** |
| Курс | **4** |
| Семестр | **7,8** |

Астрахань, 2024

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

**1.1. Целью** изучения дисциплины «Проектирование и эксплуатация защищенных информационных систем» является получение студентами прочных теоретических знаний и твердых практических навыков в области проектирования и эксплуатации защищенных информационных систем с средств моделирования информационных процессов и систем.

**1.2. Задачи освоения дисциплины:**

• определение места системы защиты информации в корпоративной информационной системе;

• определение и классификация методов защиты информации в распределенной вычислительной сети предприятия;

• раскрытие принципов, методов и технологии проектирования систем защиты информации для корпоративных информационных систем;

• изучение научных, прикладных и методологических аспектов организации технологии защиты автоматизированных систем;

• изучение научных и прикладных аспектов организации защищенной инфраструктуры корпоративной информационной системы;

• закрепление полученных знаний с целью их применения на практике после окончания учебы.

## 2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП

2.1. **Учебная дисциплина** «Проектирование и эксплуатация защищенных информационных систем» относится к элективным дисциплинам учебного плана.

**2.2. Для изучения данной учебной дисциплины (модуля) необходимы следующие знания, умения и навыки, формируемые предшествующими учебными дисциплинами:**

- Информатика.
- Основы информационной безопасности.
- Аппаратные средства вычислительной техники.
- Организационное и правовое обеспечение информационной безопасности.
- Техническая защита информации.
- Информационные технологии в управлении проектами.
- Безопасность сетей на базе Microsoft Windows Server.
- Технологии и методы программирования.
- Основы управленческой деятельности.
- Производственная практика.

В результате освоения этих дисциплин, студент должен:

знать:

– основные понятия информатики,

– принципы построения информационных систем,

- организационно-производственную структуру организации (НИИ, КБ);
- принципы и методы проектирования систем защиты информации;

уметь:

- использовать программные и аппаратные средства персонального компьютера,
- классифицировать возможные угрозы информационной безопасности;
- пользоваться нормативными документами по защите информации.

владеть:

- навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.),

- методами и средствами выявления угроз безопасности автоматизированным системам,
- навыками самостоятельного планирования и проведения проектных работ (научного исследования);
- методами расчета и анализа характеристик систем защиты информации.

**2.3. Последующие учебные дисциплины (модули) и (или) практики, для которых необходимы знания, умения, навыки, формируемые данной учебной дисциплиной (модулем):**

Навыки, приобретенные студентами при освоении дисциплины «Проектирование и эксплуатация защищенных информационных систем», помогут студентам при реализации задач преддипломной практики и написании бакалаврской работы.

## 3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Процесс освоения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОПОП ВО по данному направлению подготовки (специальности):

а) профессиональных (ПК): Способен выполнять работы по установке, настройке и техническом у обслуживанию защищенных технических средств обработки информации (ПК – 2); Способен осуществлять внедрение систем защиты информации для обеспечения информационной безопасности автоматизированных систем (ПК – 4).

**Таблица 1 – Декомпозиция результатов обучения**

| Код и наименование компетенции | Планируемые результаты обучения по дисциплине (модулю) | | |
|---|---|---|---|
| | Знать (1) | Уметь (2) | Владеть (3) |
| ПК-2 – способен выполнять работы по установке, настройке и техническом у обслуживанию защищенных технических средств обработки информации | ПК 2.1. Знать: технические описания и инструкции по эксплуатации технических средств обработки информации в защищенном исполнении, методы контроля защищенности информации от несанкционированного доступа и специальных программных воздействий, порядок аттестации объектов информатизации на соответствие требованиям безопасности информации | ПК 2.2. Уметь: проводить настройку защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами, Проводить техническое обслуживание защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-технической документацией. | ПК 2.3. Владеть: методами защиты информации от несанкционированного доступа и специальных программных воздействий на нее |
| ПК-4 – способен осуществлять внедрение систем защиты информации для обеспечения информационной безопасности автоматизированных систем | ПК-4.1. Знать: основные угрозы безопасности информации и модели нарушителя в автоматизированных системах, содержание эксплуатационной документации автоматизированной системы, типовые средства, методы и протоколы идентификации, аутентификации и авторизации основные меры по защите | ПК-4.2. Уметь: администрировать программные средства системы защиты информации автоматизированных систем, устранять известные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации, применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации, определять параметры | ПК-4.3. Владеть: методикой анализа структурных и функциональных схем защищенной автоматизированной системы |

| | | | |
|---|---|---|---|
| | информации в автоматизированных системах, нормативные правовые акты в области защиты информации | настройки программного обеспечения системы защиты информации автоматизированной системы | |

## 4. Структура и содержание дисциплины (модуля)

Общая трудоемкость дисциплины в соответствии с учебным планом составляет 6 зачетных единиц (216 часа).

Трудоемкость отдельных видов учебной работы студентов очной и очно-заочной формы обучения приведена в таблице 2.1.

**Таблица 2.1. Трудоемкость отдельных видов учебной работы по формам обучения**

| Вид учебной и внеучебной работы | для очной формы обучения |
|---|---|
| Объем дисциплины в зачетных единицах | 6 |
| Объем дисциплины в академических часах | 216 |
| Контактная работа обучающихся с преподавателем (всего), в том числе (час.): | 109,25 |
| - занятия лекционного типа, в том числе: | 36 |
| - практическая подготовка (если предусмотрена) | |
| - занятия семинарского типа (семинары, практические, лабораторные), в том числе: | 72 |
| - практическая подготовка (если предусмотрена) | |
| - в ходе подготовки и защиты курсовой работы | |
| - консультация (предэкзаменационная) | 1 |
| - промежуточная аттестация по дисциплине | 0,25 |
| Самостоятельная работа обучающихся (час.) | 106,75 |
| Форма промежуточной аттестации обучающегося (зачет/экзамен), семестр (ы) | зачет – 7 семестр; экзамен – 8 семестр |

Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий и самостоятельной работы, для каждой формы обучения представлено в таблице 2.2.

***для очной формы обучения***

| Раздел, тема дисциплины (модуля) | Контактная работа, час. | | | | | | | СР, час. | Итого часов | Форма текущего контроля успеваемости, форма промежуточной аттестации |
|---|---|---|---|---|---|---|---|---|---|---|
| | Л | | ПЗ | | ЛР | | КР / КП | | | |
| | Л | в т.ч. ПП | ПЗ | в т.ч. ПП | ЛР | в т.ч. ПП | | | | |
| **Семестр 7.** | | | | | | | | | | |
| *Тема 1. Введение. Основные принципы построения системы защиты информации корпоративной* | ***3*** | | | | ***6*** | | | ***9*** | ***18*** | Устный опрос, доклад-презентация |

| Раздел, тема дисциплины (модуля) | Контактная работа, час. | | | | | | | СР, час. | Итого часов | Форма текущего контроля успеваемости, форма промежуточной аттестации |
|---|---|---|---|---|---|---|---|---|---|---|
| | Л | | ПЗ | | ЛР | | КР / КП | | | |
| | Л | в т.ч. ПП | ПЗ | в т.ч. ПП | ЛР | в т.ч. ПП | | | | |
| *информационной системыв защите.* | | | | | | | | | | , анализ «проблемных ситуаций» |
| *Тема 2. Концепция методологии функционального моделирования.* | ***3*** | | | | ***6*** | | | ***9*** | ***18*** | Устный опрос, доклад-презентация, анализ «проблемных ситуаций» |
| *Тема 3. Основные принципы построения системы защиты информации корпоративной информационной системы* | ***3*** | | | | ***6*** | | | ***9*** | ***18*** | Устный опрос, анализ «проблемных ситуаций» |
| *Тема 4. Подсистема межсетевого экранирования* | ***3*** | | | | ***6*** | | | ***9*** | ***18*** | Устный опрос, доклад-презентация, анализ «проблемных ситуаций» |
| *Тема 5. Основные схемы сетевой защиты на базе межсетевых экранов* | ***3*** | | | | ***6*** | | | ***9*** | ***18*** | Устный опрос |
| *Тема 6. Модель нарушителя. Общие критерии* | ***3*** | | | | ***6*** | | | ***9*** | ***18*** | Устный опрос, доклад-презентация |
| **Консультации** | | | | | | | | | | |
| **Контроль промежуточной аттестации** | | | | | | | | | | **Зачет** |
| **ИТОГО за 7 семестр:** | ***18*** | | | | ***36*** | | | ***54*** | ***108*** | |
| ***Семестр 8.*** | | | | | | | | | | |
| *Тема 7. Техническое проектирование и реализация систем защиты АС* | ***4*** | | | | ***7*** | | | ***10*** | ***21*** | Устный опрос, доклад-презентация |
| *Тема 8. Анализ и оценка рисков информационной безопасности. Часть 1* | ***4*** | | | | ***8*** | | | ***12*** | ***24*** | Устный опрос, анализ «проблемных ситуаций» |
| *Тема 9. Анализ и оценка рисков информационной безопасности. Часть 2.* | ***4*** | | | | ***8*** | | | ***12*** | ***24*** | Устный опрос, анализ «проблемных ситуаций» |

| Раздел, тема дисциплины (модуля) | Контактная работа, час. | | | | | | | СР, час. | Итого часов | Форма текущего контроля успеваемости, форма промежуточной аттестации |
|---|---|---|---|---|---|---|---|---|---|---|
| | Л | | ПЗ | | ЛР | | КР / КП | | | |
| | Л | в т.ч. ПП | ПЗ | в т.ч. ПП | ЛР | в т.ч. ПП | | | | |
| *Тема 10. Проектирование системы информационной безопасности* | ***3*** | | | | ***8*** | | | ***10*** | ***21*** | Устный опрос, доклад-презентация, анализ «проблемных ситуаций» |
| *Тема 11. Эксплуатация и модификация системы информационной безопасности.* | ***3*** | | | | ***5*** | | | ***10*** | ***18*** | |
| **Консультации** | | | | | | | | | ***1*** | |
| **Контроль промежуточной аттестации** | | | | | | | | | **0,25** | **Экзамен** |
| **ИТОГО за 8 семестр:** | ***18*** | | | | ***36*** | | | ***54*** | ***108*** | |

*Примечание:* Л – лекция; ПЗ – практическое занятие, семинар; ЛР – лабораторная работа; КР – курсовая работа; СР – самостоятельная работа.

**Таблица 3 – Матрица соотнесения тем/разделов учебной дисциплины/модуля и формируемых компетенций**

| *Темы, Разделы дисциплины* | *Количество часов* | *Компетенции (указываются компетенции перечисленные в п.3)* | | *Σ общее количество компетенций* |
|---|---|---|---|---|
| | | ПК-2 | ПК - 4 | |
| Введение. Основные принципы построения системы защиты информации корпоративной информационной системы | 18 | + | + | 2 |
| Концепция методологии функционального моделирования | 18 | + | + | 2 |
| Основные принципы построения системы защиты информации корпоративной информационной системы. | 18 | + | + | 2 |
| Подсистема межсетевого экранирования | 18 | + | + | 2 |
| Основные схемы сетевой защиты на базе межсетевых экранов | 18 | + | + | 2 |
| Модель нарушителя. Общие критерии | 18 | + | + | 2 |
| Техническое проектирование и реализация систем защиты АС | 21 | + | + | 2 |

| | | | | |
|---|---|---|---|---|
| Анализ и оценка рисков информационной безопасности. Часть 1 | 24 | + | + | 2 |
| Анализ и оценка рисков информационной безопасности. Часть 2. | 24 | + | + | 2 |
| Проектирование системы информационной безопасности | 21 | + | + | 2 |
| Эксплуатация и модификация системы информационной безопасности | 18 | + | + | 2 |
| ИТОГО | 108 | | | |

**Содержание дисциплины «Проектирование и эксплуатация защищенных информационных систем»**
**7 и 8 семестры**

Лекция 1. Введение. Основные принципы построения системы защиты информации корпоративной информационной системы.

Тенденции развития современных ИС. Предмет, содержание и задачи курса, методы его изучения. Теоретические основы безопасности информационных систем. Определение места системы информационной безопасности в корпоративной информационной системе (КИС). Определение и классификация методов защиты информации в корпоративной ИС. Раскрытие принципов, методов и технологии защиты информации в корпоративной ИС. Изучение научных, прикладных и методологических аспектов организации технологии защиты в корпоративных ИС. Изучение научных и прикладных аспектов организации защищенной инфраструктуры корпоративной информационной системы. Подсистемы системы информационной безопасности автоматизированной системы (АС). Виды обеспечения автоматизированных систем. Ресурсы информационных систем и их защита. Структура, назначение и функции подсистемы управления доступом. Модели разграничения доступа в информационных системах. Дискреционное управление доступом. Мандатное управление доступом. Ролевая политика безопасности. Доктрина информационной безопасности РФ. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646. Федеральный закон Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Федеральный закон Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных». Федеральный закон Российской Федерации от 29.07.2004 №98-ФЗ «О коммерческой тайне». Федеральный закон Российской Федерации от 27.12.2002 №184-ФЗ «О техническом регулировании». Федеральный закон Российской Федерации от 06.04.2011 №63-ФЗ «Об электронной подписи».

Лекция 2. Концепция методологии функционального моделирования

Методология функционального моделирования. Концепции. Иерархия диаграмм. Виды связей. Типы связей между функциями. Основы методологии моделирования потоков данных. Базовые понятия моделирования потоков данных. Основные элементы DFD. Правила построения иерархии диаграмм потоков данных. Моделирование данных: ER-модель. Извлечение информации из интервью и выделение сущностей. Идентификация связей. Идентификация атрибутов. Виды атрибутов. Дополнительные конструкции модели данных. Методология IDEF1. некоторые особенности методологии IDEF1. Объектно-ориентированный подход к разработке ИС. Инкапсуляция. Наследование. Полиморфизм.

Визуальное моделирование. Основная цель визуального моделирования. Диаграммы UML. Федеральный закон Российской Федерации от 26.07.2017 №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Положение о сертификации средств защиты информации по требованиям безопасности информации (введено в действие приказом Председателя Гостехкомиссии России от 05.01.1996 № 3. Зарегистрировано Госстандартом России в Государственном реестре 20.03.1995. (Свидетельство №РОСС RU.ООО1.О1БИОО). ГОСТ 24.103-84. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Автоматизированные системы управления. Общие положения. ГОСТ 24.104-85 Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Автоматизированные системы управления. Общие требования. ГОСТ 24.202-80. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документа «Технико-экономическое обоснование». ГОСТ 24.203-80 Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию общесистемных документов

Лекция 3. Основные принципы построения системы защиты информации корпоративной информационной системы

Криптографическая подсистема. Подсистема управления целостностью. Подсистема защиты от вредоносных программ. Назначение и функции криптографической подсистемы. Классификация шифров. Поточное и блочное шифрование. Симметричные и асимметричные криптосистемы. Схема открытого распределения симметричных ключей Диффи-Хелмана. Понятие и механизм формирования цифровой подписи. Подсистема управления целостностью. Модель контроля целостности. Резервное копирование и восстановление данных. Схемы резервного копирования. Схемы ротации носителей. Подсистема защиты от вредоносных программ. Классификация компьютерных вирусов. Программные закладки. Технология «руткитов». Методы предупреждения вирусного заражения. Методы обнаружения компьютерных вирусов. Использование облачных технологий в антивирусном ПО. ГОСТ 24.204-80. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документа «Описание постановки задачи». ГОСТ 24.205-80 Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов по информационному обеспечению. ГОСТ 24.206-80 Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов по техническому обеспечению. ГОСТ 24.207-80 Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов по программному обеспечению. ГОСТ 24.208-80 Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов стадии «Ввод в эксплуатацию». ГОСТ 24.209-80 Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов по организационному обеспечению

Лекция 4. Подсистема межсетевого экранирования

Понятие межсетевого экрана. Функция экранирования и правила фильтрации. Требования ФСТЭК к межсетевым экранам. Показатели межсетевых экранов по классам защищенности. Понятие демилитаризованной зоны. Стандартные требования к межсетевым экранам. Политика сетевой безопасности. Политика доступа к сетевым ресурсам. Политика реализации межсетевого экранирования. Основные компоненты

межсетевых экранов. ГОСТ 24.210-82 Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов по функциональной части. ГОСТ 24.211-82 Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документа «Описание алгоритма». ГОСТ 24.301-80 Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Общие требования к выполнению текстовых документов. ГОСТ 24.302-80 Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Общие требования к выполнению схем. ГОСТ 24.304-82 Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к выполнению чертежей. ГОСТ 24.703-85 Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Типовые проектные решения. Основные положения. ГОСТ 34.201-89. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем. ГОСТ 34.320- 96 Информационные технологии. Система стандартов по базам данных. Концепции и терминология для концептуальной схемы и информационной базы. ГОСТ 34.321- 96 Информационные технологии. Система стандартов по базам данных. Эталонная модель управления данными. ГОСТ 34.601 – 90 Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания. ГОСТ 34.602-89. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Техническое задание на создание автоматизированной системы. ГОСТ 34.603-92. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Виды испытаний автоматизированных систем

Лекция 5. Основные схемы сетевой защиты на базе межсетевых экранов

Фильтрация пакетов данных между сегментами сети. Критерии фильтрации пакетов данных. Обмен электронной почтой между внутренним и внешним SMTP-серверами: правила фильтрации. Настройка правил фильтрации пакетов, поступающих из сети Интернет. Фильтрующие маршрутизаторы. Шлюзы прикладного уровня. Основные типы межсетевых экранов: программно-аппаратные, программные. Пример настройки программно-аппаратного межсетевого экрана: CheckPoint UTM-1. Пример настройки программного межсетевого экрана: Microsoft ISA Server 2006. Пример настройки программного межсетевого экрана: Microsoft ForeFront Threat Managtment Gateway 2010. Особенности межсетевых экранов нового поколения. Определение UTM. Примерная политика сетевой безопасности. ГОСТ 6.01.1-87. Единая система классификации и кодирования технико-экономической информации. Стандарт ISO/IEC 12207:1995 «InformationTechnology — SoftwareLifeCycleProcesses» (информационные технологии – жизненный цикл программного обеспечения), ГОСТ Р ИСО/МЭК 12207-99. ГОСТ Р ИСО/МЭК 15288-2005. Системная инженерия. Процессы жизненного цикла систем. ГОСТ Р ИСО/МЭК ТО 16326-2002. Программная инженерия. Руководство по применению ГОСТ Р ИСО/МЭК 12207 при управлении проектом. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения». ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».

Лекция 6. Модель нарушителя. Общие критерии

Классификация внутренних нарушителей в соответствии с РД Гостехкомиссии и ФСТЭК. Каналы несанкционированного доступа к информации. Построение модели угроз. Причины и источники появления угроз. Идентификация угроз. Классификация

уязвимостей. Классификация защищенности средств вычислительной техники. Классификация защищенности автоматизированных систем. Классификация защищенности межсетевых экранов. Новое поколение стандартов ИБ: Общие критерии. Цель разработки и структура общих критериев. Механизм описания требований к безопасности. Структура профиля защиты по общим критериям. Содержания задания по безопасности. Функциональные требования к безопасности. Требования доверия к безопасности. ГОСТ Р 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения». ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования». ГОСТ Р ИСО/МЭК 15408-1-2008 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1: Введение и общая модель», Госстандарт России. ГОСТ Р ИСО/МЭК 15408-2-2008 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2: Функциональные требования безопасности», Госстандарт России. ГОСТ Р ИСО/МЭК 15408-3-2008 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3: Требования доверия к безопасности», Госстандарт России. ГОСТ Р ИСО ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности».

Лекция 7. Техническое проектирование и реализация систем защиты АС

Жизненный цикл корпоративной информационной системы. Классификация подходов к проектированию и реализации информационной системы. Понятие встроенной и добавочной защиты. Результаты проектирования информационной системы. Состав комплекта организационно-распорядительной документации. Обязательные разделы политики безопасности информационной системы. Экономические аспекты информационной безопасности. Порядок аттестации автоматизированных систем по требованиям информационной безопасности. ГОСТ Р ИСО/МЭК 29100-2013 «Информационная технология. Методы и средства обеспечения безопасности. Основы обеспечения приватности». Рекомендации по стандартизации Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации. (утв. Приказом Ростехрегулирования от 06.04.2005 N 77-ст). Рекомендации по стандартизации Р 50.1.056-2005. Техническая защита информации. Основные термины и определения. (утв. Приказом Ростехрегулирования от 29.12.2005 N 479-ст). ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности». ГОСТ Р ИСО/МЭК 29100-2013 «Информационная технология. Методы и средства обеспечения безопасности. Основы обеспечения приватности». ГОСТ Р ИСО/МЭК 18028-1-2008 «Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность информационных технологий. Менеджмент сетевой безопасности», Госстандарт России.

Лекция 8. Анализ и оценка рисков информационной безопасности. Часть 1

Обзор стандартов по оценке рисков. Организационные стандарты по ИБ в РФ. Взаимосвязь организационных стандартов. Анализ основных положений стандарта ГОСТ Р ИСО/МЭК 27001-2006 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности». Нормативные требования к системе

управления информационной безопасности (СУИБ). Процессный поход и фазу управления рисками. Общие требования к методикам оценки и анализа рисков. Понятие инцидента ИБ. Понятие информационного актива. Угроза информационной безопасности. Понятие уязвимости. Этапы оценки рисков информационной безопасности. ГОСТ Р ИСО/МЭК ТО 19791-2008. «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем», Госстандарт России. ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования», Госстандарт России. ГОСТ Р ИСО/МЭК 27005-2009 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности», Госстандарт России. Гостехкомиссия России. Руководящий документ. Концепция защиты СВТ и АС от несанкционированного доступа к информации. М.: 1992. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. М.: 1992. Гостехкомиссия России. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. М.: 1992.

Лекция 9. Анализ и оценка рисков информационной безопасности. Часть 2.

Предварительный этап анализа рисков. Идентификация активов. Анализ угроз. Идентификация рисков ИБ. Идентификация угроз ИБ. Идентификация существующих способов управления рисками ИБ. Классификация уязвимостей по уровню критичности. Классификация уязвимостей по вероятности реализации. Оценка рисков. Количественная и качественная оценка рисков ИБ. Комбинированный полуколичественный подход к количественной оценке рисков ИБ. Пример шкалы для получения оценок активов. Пример шкалы оценки вероятностей реализации сценариев инцидентов ИБ. Детальная оценка риска информационной безопасности. Определение ранжированных значений величины риска. План управления рисками. Обработка рисков. Непрерывные действия по управлению рисками. Выбор и проверка защитных мер. Основные нормативные документы по управлению рисками информационной безопасности. Основные положения ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности». Основные положения ГОСТ Р И СОМ ЭК 27002-2012 «Информационная технология, Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. Руководящий документ 50-34.698-90 «Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов». Нормативно-методический документ «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К), (приложение к приказу Гостехкомиссии России от 30.08.2002 № 282). Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения», 1992.

Лекция 10. Проектирование системы информационной безопасности

Виды работ, выполняемых при проектировании системы безопасности. Предпроектное обследование объекта. Стадии проектирования. Выборка методов и средств

проектирования. Составление организационно-распорядительной документации. Руководство пользователя по средствам безопасности. Руководство администратора по средствам безопасности. Администрирование средств безопасности. Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», 1992. Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей», 1999. Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»,1996

Лекция 11. Эксплуатация и модификация системы информационной безопасности

Эксплуатация системы информационной безопасности АИС. Задачи и методы их решения. Основные понятия и классификация технологических процессов обработки данных. Системное администрирование АИС и администрирование безопасности АИС. Аудит информационной безопасности. Правовые и методологические основы аудита информационной безопасности. Методы оценивания информационной безопасности. Исследование полученных оценок информационной безопасности. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Приложение к Приказу ФСТЭК России от 11 февраля 2013 г. № 17. Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды. Приложение к Приказу ФСТЭК России от 14 марта 2014 г. № 31. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Приложение к Приказу ФСТЭК России от 18 февраля 2013 г. № 21. Требованиями к системам обнаружения вторжений. Приложение к Приказу ФСТЭК России от 6 декабря 2011 г. № 638. Меры защиты информации в государственных информационных системах. Методический документ ФСТЭК России от 11 февраля 2014 года. Требования о защите информации, содержащейся в информационных системах общего пользования. Приложение к Приказу Приказу ФСБ России, ФСТЭК России от 31 августа 2010 г. N 416/489.

## 5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРЕПОДАВАНИЮ И ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

### 5.1. Указания для преподавателей по организации и проведению учебных занятий по дисциплине (модулю)

**Примерная тематика лабораторно-практических работ**

Создание контекстной диаграммы.
Создание информационной модели предметной области.
Создание диаграммы IDEF1X.
Создание диаграммы DFD.
Создание организационной диаграммы.
Создание логического уровня модели данных

Связывание модели процессов и модели данных

Создание физической модели данных

Создание и настройка подсистемы антивирусной защиты защищенной информационной системы предприятия

Построение подсистемы межсетевого экранирования для системы защиты информации автоматизированной информационной системы предприятия

Установка и использование Microsoft Baseline Security Analyzer

Установка и настройка системы управления обновлениями WSUS

Организация комплекса средств защиты ОС Linux

Установка и сканирование сети при помощи сетевого сканера Xspider

При подготовке к лабораторным занятиям необходимо воспользоваться учебно-методической литературой из п.8.

### 5.2. Указания для обучающихся по освоению дисциплины (модулю)

Во время самостоятельной работы необходимо воспользоваться учебно-методической литературой из п.8.

**Таблица 4 – Содержание самостоятельной работы обучающихся**

***для очной формы обучения***

| *Темы/вопросы, выносимые на самостоятельное изучение* | *Кол-во часов* | *Формы работы* |
|---|---|---|
| Тема1. Раскрытие принципов, методов и технологии защиты информации в корпоративной ИС. Изучение научных, прикладных и методологических аспектов организации технологии защиты в корпоративных ИС. Изучение научных и прикладных аспектов организации защищенной инфраструктуры корпоративной информационной системы. | 9 | Внеаудиторная, изучение учебных пособий |
| Тема 2. Основы методологии моделирования потоков данных. Базовые понятия моделирования потоков данных. Основные элементы DFD. Правила построения иерархии диаграмм потоков данных. Моделирование данных: ER-модель. Извлечение информации из интервью и выделение сущностей. Идентификация связей. Идентификация атрибутов. Виды атрибутов. | 9 | Внеаудиторная, изучение учебных пособий |
| Тема 3. Классификация шифров. Поточное и блочное шифрование. Симметричные и асимметричные криптосистемы. Схема открытого распределения симметричных ключей Диффи-Хелмана. Классификация компьютерных вирусов. Программные закладки. Технология | 9 | Внеаудиторная, изучение учебных пособий |

| | | |
|---|---|---|
| «руткитов». Методы предупреждения вирусного заражения. Методы обнаружения компьютерных вирусов. | | |
| Тема 4. Показатели межсетевых экранов по классам защищенности. Понятие демилитаризованной зоны. Стандартные требования к межсетевым экранам. Политика сетевой безопасности. Политика доступа к сетевым ресурсам. | 9 | Внеаудиторная, изучение учебных пособий, изучение нормативно-правовых документов |
| Тема 5. Пример настройки программно-аппаратного межсетевого экрана: CheckPoint UTM-1. Пример настройки программного межсетевого экрана: Microsoft ISA Server 2006. Пример настройки программного межсетевого экрана: Microsoft ForeFront Threat Managtment Gateway 2010. Особенности межсетевых экранов нового поколения. Определение UTM. Примерная политика сетевой безопасности. | 9 | Внеаудиторная, изучение учебных пособий |
| Тема 6. Новое поколение стандартов ИБ: Общие критерии. Цель разработки и структура общих критериев. Механизм описания требований к безопасности. Структура профиля защиты по общим критериям. Содержания задания по безопасности. Функциональные требования к безопасности. Требования доверия к безопасности. | 9 | Внеаудиторная, изучение учебных пособий, изучение нормативно-правовых документов |
| Тема 7. Экономические аспекты информационной безопасности. Порядок аттестации автоматизированных систем по требованиям информационной безопасности. | 10 | Внеаудиторная, изучение учебных пособий, изучение нормативно-правовых документов |
| Тема 8. Системы менеджмента информационной безопасности». Нормативные требования к системе управления информационной безопасности (СУИБ). Процессный поход и фазу управления рисками. | 12 | Внеаудиторная, изучение учебных пособий, изучение нормативно-правовых документов |
| Тема 9. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности». Основные положения ГОСТ Р ИСО МЭК 27002-2012 «Информационная технология, Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. | 12 | Внеаудиторная, изучение учебных пособий, изучение нормативно-правовых документов |
| Тема 10. Составление организационно- | 10 | Внеаудиторная, |

| | | |
|---|---|---|
| распорядительной документации. Руководство пользователя по средствам безопасности. Руководство администратора по средствам безопасности. Администрирование средств безопасности. | | изучение учебных пособий |
| Тема 11. Аудит информационной безопасности. Правовые и методологические основы аудита информационной безопасности. Методы оценивания информационной безопасности. Исследование полученных оценок информационной безопасности. | 10 | Внеаудиторная, изучение учебных пособий |

**5.3. Виды и формы письменных работ, предусмотренных при освоении дисциплины (модуля), выполняемые обучающимися самостоятельно**

Учебный проект может содержать следующие разделы и части:
Титульный лист
Задание на учебный проект
Реферат
Содержание
Введение
1 Анализ и выбор метода решения задачи «Проектирование защищенной информационной системы для решения задачи «***Наименование прикладной задачи или подсистемы автоматизированной системы управления***»»
1.1 Технико-экономическая характеристика предприятия (если задача решается для предприятия)
1.2 Актуальность выбранной темы
1.3 Анализ информационных потоков и определение требований к обеспечению их безопасности
1.4 Анализ технических и программных средств, используемых для решения задачи (или подсистемы)
1.5 Характеристика методов, средств и систем информационной безопасности используемых для решения задачи (или подсистемы)
1.6 Постановка задачи проектирования защищенной информационной системы для решения задачи (подсистемы)
2 Проектирование защищенной информационной системы для решения задачи «***Наименование прикладной задачи или подсистемы автоматизированной системы управления***»»
2.1 Основные положения проектирования защищенной информационной системы для решения задачи «***Наименование прикладной задачи или подсистемы автоматизированной системы управления***»
2.2 Разработка нормативной базы использования методов, средств и систем информационной безопасности при проектировании защищенной информационной системы
2.3 Разработка модели угроз информационной безопасности, возникающих при решении задачи «Наименование прикладной задачи или подсистемы автоматизированной системы управления»
2.4 Оценка и анализ рисков информационной безопасности при решении задачи «Наименование прикладной задачи или подсистемы автоматизированной системы управления»

2.5 Обоснование выбора аппаратных средств защиты информации

2.6 Обоснование выбора программных средств защиты информации

2.7 Разработка структуры защищенной информационной системы для решения задачи «***Наименование прикладной задачи или подсистемы автоматизированной системы управления***»

2.8 Разработка и моделирование структуры информационной базы данных

2.9 Разработка информационно-логической модели системы

Заключение

Список использованных источников

Приложения

**Названия пунктов должны быть привязаны к конкретному учебному проекту. Количество разделов и их формулировки могут изменяться.**

**В приложения** выносятся нормативные документы, формы, схемы, распечатки кодов программ и параметров настройки средств защиты информации.

Рассмотрим содержание перечисленных разделов учебного проекта.

**Введение**

Введение должно содержать общие сведения об учебном проекте, отражать цели и задачи разработки проекта, объект и технические требования на которые он ориентирован. Целями проекта могут быть: разработка защищенной информационной системы, либо анализ и модификация существующей системы информационной безопасности. В рамках учебного проекта может быть выполнена разработка отдельных программных модулей, либо настройка средств защиты информации на конкретные условия применения.

Объем введения не должен превышать 2-3 страниц.

**Анализ и выбор метода решения «Проектирование защищенной информационной системы для решения задачи «Наименование прикладной задачи или подсистемы автоматизированной системы управления»»**

**В параграфе 1.1** необходимо дать краткую характеристику технико-экономических параметров объекта, охарактеризовать основные функции и задачи стоящие перед предприятием (организацией). Здесь же может быть приведена организационная структура предприятия, с указанием организационных связей и основных задач, стоящих перед подразделениями.

**В параграфе 1.2** производится анализ основных информационных потоков на предприятии. При этом должна быть выполнена классификация информации по уровню конфиденциальности и определен уровень соответствия полученной классификации, существующей на предприятии. В случае наличия принципиальных различий в классификациях необходимо попытаться определить, чем вызваны соответствующие расхождения.

**В параграфе 1.3** рассматривается комплекс программных и аппаратных средств, используемых на предприятии. Особое внимание должно быть уделено структуре локальной сети и используемых в рамках этой сети технологий обработки, передачи и хранения информации.

**Параграф 1.4** характеризует комплекс методов, средств и систем информационной безопасности, используемых на предприятии. Параграф должен представлять собой критический анализ всего комплекса средств. При этом могут показываться не только недостатки, но и достоинства тех или иных средств. Если имеется возможность, делаются ссылки на регламентирующие документы и инструкции, которые приводятся в приложении.

**В параграфе 1.5** требуется обосновать необходимость защищенной информационной системы для решения стоящей перед студентом задачи. Здесь необходимо привести основные недостатки существующей системы. При этом следует

отметить те недостатки, устранение которых планируется в рамках учебного проекта. К наиболее характерным недостаткам можно отнести:

- перечень угроз, защита от которых не предусмотрена в рамках существующей системы защиты информации;
- использование в существующей системе устаревших программно-аппаратных компонентов;
- несовершенство процессов контроля состояния системы;
- большая трудоемкость в организации тех или иных мероприятий по защите данных.

В параграфе также рекомендуется обосновать выбор технологии проектирования, для разработки программных модулей.

**Проектирование защищенной информационной системы для решения задачи «Наименование прикладной задачи или подсистемы автоматизированной системы управления»**

**В параграфе 2.1** дается краткая характеристика элементов защищенной информационной системы, выбранных для реализации в рамках учебного проекта. При этом приводится обоснование сделанного выбора.

**Параграф 2.2** раскрывает перечень организационных мероприятий, разработанных реализации проекта «**Проектирование защищенной информационной системы для решения задачи «Наименование прикладной задачи или подсистемы автоматизированной системы управления»».**

При этом необходимо разработать перечень всей нормативной документации (планы, графики, инструкции) для всех предлагаемых мероприятий. Примеры данных документов могут быть приведены в приложениях.

**В параграфе 2.3** рассматриваются технические средства, предлагаемые для использования в рамках проектируемой системы. При этом должен быть приведен сравнительный анализ близких по функциональным возможностям устройств и обоснован выбор того или иного аппаратного комплекса. Кроме этого должны быть представлены основные настройки аппаратной части и описаны основные режимы работы выбранного оборудования.

**Параграф 2.4** должен описывать программные средства, для защиты информации, планируемые для использования в рамках проектируемой системы. Здесь также должен быть проведен сравнительный анализ близких по функциональному назначению программных средств. Особое внимание должно быть уделено требованиям к техническому обеспечению и подготовке обсуживающего персонала. Также, в этом параграфе должны быть рассмотрены возможные способы взаимодействия аппаратных и программных средств защиты информации.

**В параграфе 2.5.1** должно быть приведено обоснование необходимости разработки дополнительного программного обеспечения. Следует уделить внимание существующим программно-аппаратным комплексам, призванным решать аналогичные задачи и указать на причины, по которым данные продукты не могут быть использованы. Типичными причинами могут являться:

- высокая стоимость существующих решений;
- отсутствие комплексов реализующих данную функцию;
- узость задачи или набор определенных специфических требований.

**Параграф 2.5.2** содержит информационно-логическую модель проектируемой информационной системы. Должен быть представлен общий алгоритм работы программы, проведен анализ входной и выходной информации. Разрабатываются системы кодирования информации и структуры массивов, баз данных. Здесь же может быть приведено обоснование выбора платформы разработки и набора технических средств.

**В параграфе 2.5.3** приводится развернутая схема функционирования проектируемой информационной системы программного обеспечения, с представлением нескольких

макетов входных и выходных форм. Описываются выходные документы, формы которых представляются в приложении.

**В заключении** помещаются выводы, сделанные по учебному проекту, направления внедрения проекта, перспективы дальнейшего совершенствования системы информационной безопасности.

**В списке использованных источников** следует литературные источники, использованные при разработке проекта и при написании пояснительной записки, а также нормативные документы, которыми руководствовался автор проекта. В тексте дипломного проекта следует приводить ссылки на все использованные источники. Список использованных источников оформляется в соответствии со стандартом «ГОСТ 7.1-2003 Библиографическая запись. Библиографическое описание. Общие требования и правила составления», для оформление ссылок на электронные ресурсы следует руководствоваться «ГОСТ 7.82-2001 Библиографическая запись. Библиографическое описание электронных ресурсов».

## 6. ОБРАЗОВАТЕЛЬНЫЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

При реализации различных видов учебной работы по дисциплине могут использоваться электронное обучение и дистанционные образовательные технологии.

В соответствии с требованиями ФГОС ВО по направлению подготовки бакалавров в рамках изучения дисциплины «Проектирование и эксплуатация защищенных информационных систем» предусмотрено использование в учебном процессе в течение одного семестра следующих активных и интерактивных форм проведения занятий:

### 6.1. Образовательные технологии

**Таблица 5 – Образовательные технологии, используемые при реализации учебных занятий**

| Раздел, тема дисциплины (модуля) | Форма учебного занятия | | |
|---|---|---|---|
| | Лекция | Практическое занятие, семинар | Лабораторная работа |
| Введение. Основные принципы построения системы защиты информации корпоративной информационной системы | *Обзорная лекция* | *Не предусмотрено* | *Фронтальный опрос* |
| Концепция методологии функционального моделирования. | *Лекция-диалог* | *Не предусмотрено* | *Тематические дискуссии, анализ конкретных ситуаций* |
| Основные принципы построения системы защиты информации корпоративной информационной системы | *Лекция* | *Не предусмотрено* | *Выполнение практических заданий, тематические дискуссии* |
| Подсистема межсетевого экранирования | *Лекция* | *Не предусмотрено* | *Выполнение практических заданий,* |

| | | | |
|---|---|---|---|
| | | | *тематические дискуссии* |
| Основные схемы сетевой защиты на базе межсетевых экранов | *Обзорная лекция* | *Не предусмотрено* | *Фронтальный опрос* |
| Модель нарушителя. Общие критерии | *Лекция-диалог* | *Не предусмотрено* | *Фронтальный опрос, выполнение практических заданий, тематические дискуссии* |
| Техническое проектирование и реализация систем защиты АС | *Лекция* | *Не предусмотрено* | *Тематические дискуссии, анализ конкретных ситуаций* |
| Анализ и оценка рисков информационной безопасности. Часть 1 | *Лекция-диалог* | *Не предусмотрено* | *Фронтальный опрос* |
| Анализ и оценка рисков информационной безопасности. Часть 2. | *Лекция* | *Не предусмотрено* | *Фронтальный опрос* |
| Проектирование системы информационной безопасности | *Лекция* | *Не предусмотрено* | *Тематические дискуссии, анализ конкретных ситуаций* |
| Эксплуатация и модификация системы информационной безопасности. | *Лекция-диалог* | *Не предусмотрено* | *Фронтальный опрос* |

Учебные занятия по дисциплине могут проводиться с применением информационно-телеком-муникационных сетей при опосредованном (на расстоянии) интерактивном взаимодействии обучающихся и преподавателя в режимах on-line в формах: видеолекций, лекций-презентаций, видеоконференции, собеседования в режиме чат, форума, чата, выполнения виртуальных практических и/или лабораторных работ и др.

Максимальный объем занятий обучающегося с применением электронных образовательных технологий не должен превышать 25%.

| Название образовательной технологии | Темы, разделы дисциплины | Краткое описание применяемой технологии |
|---|---|---|
| Сдача практических работ | Разделы 1 – 11 | Проведение входного, текущего и рейтингового контроля знаний учащихся (в системах дистанционного обучения) |
| Консультации по электронной почте | Разделы 1 - 11 | Подготовка к защите рефератов и учебных проектов (адрес электронной почты akhanova@mail.ru). |

| | | |
|---|---|---|
| Активная лекция | Основные схемы сетевой защиты на базе межсетевых экранов | Лекция-визуализация |
| Активная лекция | Техническое проектирование и реализация систем защиты АС | Лекция-визуализация |

### 6.2. Информационные технологии

При реализации различных видов учебной и внеучебной работы используются следующие информационные технологии:

- использование возможностей Интернета в учебном процессе (использование информационного сайта преподавателя (рассылка заданий, предоставление выполненных работ, ответы на вопросы, ознакомление учащихся с оценками и т.д.));
- использование электронных учебников и различных сайтов (например, электронные библиотеки, журналы и т.д.) как источников информации;
- использование возможностей электронной почты преподавателя;
- использование средств представления учебной информации (электронных учебных пособий и практикумов, применение новых технологий для проведения очных (традиционных) лекций и семинаров с использованием презентаций и т.д.);
- использование интегрированных образовательных сред, где главной составляющей являются не только применяемые технологии, но и содержательная часть, т.е. информационные ресурсы (доступ к мировым информационным ресурсам, на базе которых строится учебный процесс);
- использование виртуальной обучающей среды (или системы управления обучением LMS Moodle «Электронное образование») или иных информационных систем, сервисов и мессенджеров

### 6.3. Перечень программного обеспечения и информационных справочных систем

#### 6.3.1. Программное обеспечение:

| Наименование программного обеспечения | Назначение |
|---|---|
| Adobe Reader | Программа для просмотра электронных документов |
| Mozilla FireFox | Браузер |
| Microsoft Office 2013, Microsoft Office Project 2013, Microsoft Office Visio 2013 | Офисная программа |
| 7-zip | Архиватор |
| Microsoft Windows 7 Professional | Операционная система |

| | |
|---|---|
| Kaspersky Endpoint Security | Средство антивирусной защиты |
| Платформа дистанционного обучения LMS Moodle | Виртуальная обучающая среда |

**6.3.2. Современные профессиональные базы данных и информационные справочные системы:**

1. Электронный каталог Научной библиотеки АГУ на базе MARK SQL НПО «Информ-систем»: https://library.asu.edu.ru.
2. Электронный каталог «Научные журналы АГУ»: http://journal.asu.edu.ru/.
3. Универсальная справочно-информационная полнотекстовая база данных периодических изданий ООО «ИВИС»: http://dlib.eastview.com/
4. Электронно-библиотечная система elibrary. http://elibrary.ru
5. Справочная правовая система КонсультантПлюс: http://www.consultant.ru
6. Информационно-правовое обеспечение «Система ГАРАНТ»: http://garant-astrakhan.ru

## 7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

### 7.1. Паспорт фонда оценочных средств

При проведении текущего контроля и промежуточной аттестации по дисциплине (модулю) «Проектирование и эксплуатация защищенных информационных систем» проверяется сформированность у обучающихся компетенций, указанных в разделе 3 настоящей программы. Этапность формирования данных компетенций в процессе освоения образовательной программы определяется последовательным освоением дисциплин (модулей) и прохождением практик, а в процессе освоения дисциплины (модуля) – последовательным достижением результатов освоения содержательно связанных между собой разделов, тем.

**Таблица 6 – Соответствие разделов, тем дисциплины (модуля), результатов обучения по дисциплине (модулю) и оценочных средств**

| № п/п | Контролируемые разделы (темы) дисциплины* | Код контролируемой компетенции (или ее части) | Наименование оценочного средства |
|---|---|---|---|
| 1. | Введение. Основные принципы построения системы защиты информации корпоративной информационной системы | ПК-2, ПК-4 | Входное тестирование |
| 2. | Концепция методологии функционального моделирования. | ПК-2, ПК-4 | Отчет по лабораторной работе 1<br>Контрольная работа 1<br>Опрос на экзамене |
| 3. | Основные принципы построения системы защиты информации корпоративной информационной системы | ПК-2, ПК-4 | Отчет по лабораторной работе 2<br>Контрольная работа 2<br>Опрос на экзамене |
| 4. | Подсистема межсетевого экранирования | ПК-2, ПК-4 | Отчет по лабораторной работе 3<br>Контрольная работа 3 |

| | | | |
|---|---|---|---|
| | | | Опрос на экзамене |
| 5. | Основные схемы сетевой защиты на базе межсетевых экранов | ПК-2, ПК-4 | Отчет по лабораторной работе 4<br>Контрольная работа 4<br>Опрос на экзамене |
| 6. | Модель нарушителя. Общие критерии | ПК-2, ПК-4 | Промежуточное тестирование |
| 7. | Техническое проектирование и реализация систем защиты АС | ПК-2, ПК-4 | Отчет по лабораторной работе 5<br>Контрольная работа 5<br>Опрос на экзамене |
| 8. | Анализ и оценка рисков информационной безопасности. Часть 1 | ПК-2, ПК-4 | Отчет по лабораторной работе 6<br>Контрольная работа 6<br>Опрос на экзамене |
| 9. | Анализ и оценка рисков информационной безопасности. Часть 2. | ПК-2, ПК-4 | Отчет по лабораторной работе 7<br>Контрольная работа 7<br>Опрос на экзамене |
| 10. | Проектирование системы информационной безопасности | ПК-2, ПК-4 | Защита учебных проектов |
| 11. | Эксплуатация и модификация системы информационной безопасности | ПК-2, ПК-4 | Итоговое тестирование |

**7.2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания**

При решении комплексной ситуационной задачи можно использовать следующие критерии оценки:

**Таблица 7 – Показатели оценивания результатов обучения в виде знаний**

| Шкала оценивания | Критерии оценивания |
|---|---|
| 5 «отлично» | демонстрирует глубокое знание теоретического материала, умение обоснованно излагать свои мысли по обсуждаемым вопросам, способность полно, правильно и аргументированно отвечать на вопросы, приводить примеры |
| 4 «хорошо» | демонстрирует знание теоретического материала, его последовательное изложение, способность приводить примеры, допускает единичные ошибки, исправляемые после замечания преподавателя |
| 3 «удовлетворительно» | демонстрирует неполное, фрагментарное знание теоретического материала, требующее наводящих вопросов преподавателя, допускает существенные ошибки в его изложении, затрудняется в приведении примеров и формулировке выводов |
| 2 «неудовлетворительно» | демонстрирует существенные пробелы в знании теоретического материала, не способен его изложить и ответить на наводящие вопросы преподавателя, не может привести примеры |

**Таблица 8 – Показатели оценивания результатов обучения в виде умений и владений**

| Шкала оценивания | Критерии оценивания |
|---|---|
| 5 «отлично» | демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы |
| 4 «хорошо» | демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы, допускает единичные ошибки, исправляемые после замечания преподавателя |
| 3 «удовлетвори тельно» | демонстрирует отдельные, несистематизированные навыки, не способен применить знание теоретического материала при выполнении заданий, испытывает затруднения и допускает ошибки при выполнении заданий, выполняет задание при подсказке преподавателя, затрудняется в формулировке выводов |
| 2 «неудовлетво рительно» | не способен правильно выполнить задание |

**7.3. Контрольные задания или иные материалы, необходимые для оценки результатов обучения по дисциплине (модулю)**

***Тема 1. Введение. Основные принципы построения системы защиты информации корпоративной информационной системы***

**1. Входное тестирование**

1. К системным программам в автоматизированных системах управления относят следующие:

А. Управляющие работой аппаратных средств и обеспечивающие услугами пользователя и его прикладные комплексы.
Б. Игры, трансляторы, компиляторы, интерпретаторы.
В. Программы, которые хранятся на жестком диске.
Г. Все ответы неверны.

2. Модель автоматизированной системы – это?

А. Множество существенных свойств, которыми система обладает в данный момент времени.
Б. Набор тестов для проверки функционирования системы в различных режимах.
В. Описание системы, отображающее определенную группу ее свойств.
Г. Перечень подсистем автоматизированной системы.

3. Совокупность данных, получаемая АСУ ТП от объекта управления – это:

А. Промежуточная информация.
Б. Входная информация.
В. Выходная информация.
Г. Основная информация.

4. Какие модели разграничения доступа используются в автоматизированных системах?

А. Модель дискреционного разграничения доступа.
Б. Модель ролевого разграничения доступа.
В. Универсальная модель разграничения доступа.
Г. Модель мандатного разграничения доступа.

5. К корпоративным информационным системам относятся следующие системы:

А. Информационные системы, осуществляющие бизнес в Интернете.
Б Информационные системы, предоставляющие услуги по доступу в Интернет.
В. Информационная системы, обеспечивающие деятельность корпораций.
Г. Статический симметричный ключ.
Д. Компьютерные сети корпораций.

6. "Общие критерии" включают следующие виды требований:

А. Функциональные требования.
Б. Требования доверия.
В. Требования эффективности.
Г. Требования к процессу проектирования.
Д. Требования неотказуемости.
Д.Все ответы неверны.

***Тема 2. «Концепция методологии функционального моделирования»***

1. ***Лабораторная работа 1.*** **«Функционально-ориентированный подход к проектированию SADT (IDEF0)»**

Методология функционального моделирования. Концептуальные положения методологии функционального моделирования: Модель, Блочное моделирование и его графическое представление, Лаконичность и точность; Передача информации; Строгость и формализм; Итеративное моделирование; Отделение «организации» от «функций».

Этапы построения модели IDEF0. Принципы методологии IDEF0. Основные понятия методологии IDEF0: работы, связи. Типы связей между функциями: вход, выход, управление, механизм.

Стратегии декомпозиции. Завершение моделирования (критерии для определения момента прекращения декомпозиции).

**Задание**

Выполнить методические указания № 1 лабораторного практикума для описания бизнес-процессов компании, специализирующейся на сборке и реализации компьютеров. Для описания использовать нотацию IDEF0

1. Создание контекстной диаграммы
2. Создание диаграммы декомпозиции
3. Создание диаграммы декомпозиции A2
4. Создание диаграммы узлов
5. Создание FEO-диаграммы
6. Расщепление и слияние моделей

**Контрольные вопросы**

1. Принципы построения модели IDEF0.

2. Работа (Activity).
3. Стрелка (Arrow).
4. Нумерация работ и диаграмм.
5. Диаграммы дерева узлов и FEO.
6. Слияние и расщепление моделей.

1. ***Рейтинговая контрольная работа 1***

Вопросы:

1. Предмет, содержание и задачи курса, методы его изучения
2. Виды обеспечения автоматизированных систем
3. Ресурсы информационных систем и их защита
4. Структура, назначение и функции подсистемы управления доступом
5. Модели разграничения доступа в информационных системах
6. Дискреционное управление доступом
7. Мандатное управление доступом
8. Ролевая политика безопасности

***Тема 3. Основные принципы построения системы защиты информации корпоративной информационной системы***

1. ***Лабораторная работа 2 Лабораторная работа №2 «Создание модели IDEF3»***

Метод описания IDEF3. Диаграммы. Единицы работ. Связи. Перекрестки. Декомпозиция работ. Описание сценария. Стоимостный анализ (Activity Based Costing – ABC). Свойства, определяемые пользователем (User Defined Properties – UDP).

**Задание**

Выполнить методические указания № 2 лабораторного практикума для описания бизнес-процессов компании, специализирующейся на сборке и реализации компьютеров. Для описания использовать нотацию IDEF3

1. Создание диаграммы IDEF3
2. Создание сценария
3. Стоимостный анализ (Activity Based Costing)
4. Использование категорий UDP

**Контрольные вопросы к лабораторной работе**

1. Метод описания процессов IDEF3
2. Диаграммы
3. Единицы работ
4. Связи
5. Перекрестки
6. Декомпозиция работ
7. Описание сценария
8. Создание смешанной модели
9. Стоимостный анализ (Activity Based Costing)
10. Свойства, определяемые пользователем (User Defined Properties)

2. ***Рейтинговая контрольная работа 2***

Вопросы:

1. Назначение и функции криптографической подсистемы.
2. Классификация шифров. Поточное и блочное шифрование.
3. Симметричные и асимметричные криптосистемы.
4. Схема открытого распределения симметричных ключей Диффи-Хелмана.

5. Понятие и механизм формирования цифровой подписи.
6. Подсистема управления целомстностью.
7. Модель контроля целостности.
8. Резервное копирование и восстановление данных.
9. Подсистема защиты от вредоносных программ.

***Тема 4. Подсистема межсетевого экранирования***

1. ***Лабораторная работа 3 «Моделирование потоков данных (процессов) (DFD)»***

Базовые понятия моделирования. Идея DFD. Основные элементы DFD: работы, внешние сущности, потоки данных, хранилища данных. Построение иерархии диаграмм потоков данных. Организационные диаграммы. Диаграммы Swim Lane.

Задание

Выполнить методические указания № 3 лабораторного практикума для описания потоков данных компании, специализирующейся на сборке и реализации компьютеров. Для описания использовать нотацию DFD

1. Создание модели TO-BE (реинжиниринг бизнес-процессов).
2. Создание диаграммы DFD
3. Создание организационной диаграммы
4. Создание диаграммы Swim Lane.

Контрольные вопросы

1. Модели AS-IS и TO-BE
2. Диаграммы потоков данных (Data Flow Diagramming)
3. Работы
4. Внешние сущности
5. Стрелки (потоки данных).
6. Хранилище данных
7. Слияние и разветвление стрелок
8. Построение диаграмм DFD
9. Нумерация объектов
10. Организационной диаграммы
11. Диаграммы Swim Lane

2. ***Рейтинговая контрольная работа 3***

**Вариант 1**

1. Понятие межсетевого экрана.
2. Функция экранирования и правила фильтрации.
3. Требования ФСТЭК к межсетевым экранам.
4. Понятие демилитаризованной зоны.

**Вариант 2**

1. Политика сетевой безопасности. Политика доступа к сетевым ресурсам.
2. Политика сетевой безопасности. Политика реализации межсетевого экранирования.
3. Основные компоненты межсетевых экранов.
4. Основные схемы сетевой защиты на базе межсетевых экранов.

***Тема 5. Основные схемы сетевой защиты на базе межсетевых экранов***

1. ***Лабораторная работа 4*** **«Связывание модели процессов и модели данных. Создание отчетов по модели данных».**

Модель данных и ее соответствие модели процессов. Экспорт данных из ERwin в BPwin и связывание объектов модели данных со стрелками и работами. Создание сущностей и атрибутов BPwin и их экспорт в ERwin. Создание отчетов по модели данных с помощью Report Browser.

**Задание**

Выполнить методические указания лабораторной работы № 2 лабораторного практикума по ERwin для связывания моделей данных и процессов компании, специализирующейся на сборке и реализации компьютеров.

1. Выполните экспорт данных из модели данных в модель процессов
2. Создайте дополнительные сущности и атрибуты в модели процессов
3. Свяжите стрелки на диаграмме процессов с импортированными и созданными сущностями и атрибутами.
4. Задокументируйте воздействия работ на данные
5. Создайте отчет Data Usage Report в модели процессов
6. Экспортируйте данные из модели процессов в модель данных
7. Создайте отчет по сущностям в ERwin с помощью Report Template Builder

**Контрольные вопросы**

1. Назначение связи объектов модели процессов и модели данных
2. Способы связывания объектов модели данных и модели процессов
3. Экспорт и импорт данных в ERWin и BPWin
4. Связывание сущности и атрибута со стрелкой. Назначение кнопок в диалоге Arrow Properties.
5. Копирование связанных данных из другой стрелки
6. Миграция данных от дочерних к родительским стрелкам.
7. Документирование воздействия работ на данные. Ассоциации для сущностей и атрибутов.
8. Отображение результата связывания объектов модели процессов
9. Редактирования сущностей и атрибутов в модели процессов
10. Назначение инструмента Report Browser
11. Инструментальная среда Report Browser
12. Редактор отчетов
13. Форматирование отчетов. Форматы экспорта
14. Создание именованного представления в Report Browser.

***Рейтинговая контрольная работа 4***

1. Классификация внутренних нарушителей в соответствии с РД Гостехкомиссии и ФСТЭК.
2. Каналы несанкционированного доступа к информации.
3. Построение модели угроз.
4. Классификация угроз. Причины появления угроз.
5. Классификация уязвимостей.
6. Классификация защищенности средств вычислительной техники.
7. Цель разработки и структура общих критериев.
8. Механизм описания требований к безопасности.
9. Структура профиля защиты по общим критериям.
10. Содержания задания по безопасности. Функциональные требования к безопасности.
11. Требования доверия к безопасности.

***Тема 6. Модель нарушителя. Общие критерии***

***Промежуточное тестирование***

1. IDEF-технологии ориентированы на поддержку:
   - *Методологии структурного анализа,*
   - *Методологии объектно-ориентированного анализа.*
2. В соответствии со стандартом ISO-IES 12207 все процессы ЖЦ ПО разделены на:
   - *Три группы – основные, организационные и бизнес процессы,*

- *Две группы – основные и вспомогательные процессы,*
- *Три группы – основные, вспомогательные и бизнес процессы,*
- *Три группы – основные, вспомогательные и организационные процессы.*

3. Какие из перечисленных процессов входят в группу «Организационные процессы ЖЦ ПО»
   - *Управление,*
   - *Обеспечение качества,*
   - *Поставка,*
   - *Аттестация,*
   - *Усовершенствование,*
   - *Создание инфраструктуры,*
   - *Документирование,*
   - *Сопровождение,*
   - *Все выше перечисленные.*
4. К настоящему времени наибольшее распространение получили следующие модели ЖЦ ПО:
   - *Структурная и спиральная модель,*
   - *Функциональная и структурная модель,*
   - *Каскадная и спиральная модель,*
   - *Каскадная и функциональная модель.*
5. Состав функциональной модели:
   - *Диаграммы и глоссарий,*
   - *Диаграммы, фрагменты текста и глоссарий,*
   - *Диаграммы, фрагменты текста и рисунки,*
   - *Диаграммы и потоки данных.*

6. Накопители данных на диаграмме потоков данных это:
   - *Абстрактное устройство для хранения информации,*
   - *База данных,*
   - *Таблица в базе данных,*
   - *Магнитный носитель.*
7. Цели моделирования данных состоит в:
   - *Визуализации потов данных,*
   - *Определение требований к системе,*
   - *Обеспечении разработчика концептуальной схемой базы данных,*
   - *Обеспечении разработчика моделью предметной области.*
8. Сколько типов диаграмм выделяют в языку UML:
   - *Девять,*
   - *Одиннадцать,*
   - *Семь,*
   - *Восемь.*
9. какие отношения возможности на диаграмме Use Case:
   - *зависимость, включения, расширения,*
   - *ассоциации, включения, расширения,*
   - *ассоциации, реализации, обобщения,*
   - *ассоциации, зависимости, обобщения.*
10. Квантор видимости операции класса может принимать следующие значения:
    - *Общедоступный,*
    - *Закрытый,*
    - *Защищенный,*

- *Секретный.*

11. Сторожевое условие на диаграмме состояний:
    - *Записывается в прямых скобках после события-триггера и представляет булевское выражение,*
    - *Записывается в круглых скобках после события-триггера и представляет булевское выражение,*
    - *Записывается в прямых скобках до события-триггера и представляет булевское выражение,*
    - *Записывается в круглых скобках до события-триггера и представляет булевское выражение.*
12. Разработка функциональных моделей (модели «как есть» и «как должно быть») позволяет:
    - *Глубоко изучить природу бизнес-процессов,*
    - *Выявить ключевые бизнес-процессы относительно целей организации процессы,*
    - *Провести реструктуризацию (реинжиниринг) старых и разработку новых процессов,*
    - *Все выше перечисленное.*
13. В соответствии со стандартном ISO/IEC 12207 основные процессы ЖЦ ПО состоят из:
    - *Пяти основных процессов (приобретение, поставка, разработка, обучение, сопровождение),*
    - *Четырех основных процессов (приобретение, поставка, эксплуатация, сопровождение),*
    - *Пяти основных процессов (приобретение, поставка, разработка, эксплуатация, сопровождение),*
    - *Четырех основных процессов (управление, создание инфраструктуры, разработка, сопровождение).*
14. Принципиальной особенностью каскадного подхода является следующие:
    - *Прикладное ПО создается не сразу, а по частям с использованием метода прототипирования,*
    - *Переход на следующую стадию осуществляется только после того, как будет полностью завершена работа на текущей стадии, и возвратов на пройденные стадии не предусматривается,*
    - *Переход на следующую стадию осуществляется только после того, как будет полностью завершена работа на текущей стадии, возвратов на пройденные стадии,*
    - *На каждой стадии формируется определенная версия ПО.*

## *Тема 7. Техническое проектирование и реализация систем защиты АС*

### 1. *Лабораторная работа 5.* «Связывание модели процессов и модели данных. Создание отчетов по модели данных».

Модель данных и ее соответствие модели процессов. Экспорт данных из ERwin в BPwin и связывание объектов модели данных со стрелками и работами. Создание сущностей и атрибутов BPwin и их экспорт в ERwin. Создание отчетов по модели данных с помощью Report Browser.

**Задание**

Выполнить методические указания лабораторной работы № 2 лабораторного практикума по ERwin для связывания моделей данных и процессов компании, специализирующейся на сборке и реализации компьютеров.

1. Выполните экспорт данных из модели данных в модель процессов

2. Создайте дополнительные сущности и атрибуты в модели процессов
3. Свяжите стрелки на диаграмме процессов с импортированными и созданными сущностями и атрибутами.
4. Задокументируйте воздействия работ на данные
5. Создайте отчет Data Usage Report в модели процессов
6. Экспортируйте данные из модели процессов в модель данных
7. Создайте отчет по сущностям в ERwin с помощью Report Template Builder

**Контрольные вопросы**

15. Назначение связи объектов модели процессов и модели данных
16. Способы связывания объектов модели данных и модели процессов
17. Экспорт и импорт данных в ERWin и BPWin
18. Связывание сущности и атрибута со стрелкой. Назначение кнопок в диалоге Arrow Properties.
19. Копирование связанных данных из другой стрелки
20. Миграция данных от дочерних к родительским стрелкам.
21. Документирование воздействия работ на данные. Ассоциации для сущностей и атрибутов.
22. Отображение результата связывания объектов модели процессов
23. Редактирования сущностей и атрибутов в модели процессов
24. Назначение инструмента Report Browser
25. Инструментальная среда зReport Browser
26. Редактор отчетов
27. Форматирование отчетов. Форматы экспорта
28. Создание именованного представления в Report Browser.

***2. Рейтинговая контрольная работа 5***

1. Жизненный цикл корпоративной информационной системы.
2. Классификация подходов к проектированию и реализации информационной системы.
3. Понятие встроенной и добавочной защиты.
4. Результаты проектирования информационной системы.
5. Состав комплекта организационно-распорядительной документации.
6. Обязательные разделы политики безопасности информационной системы.
7. Экономические аспекты информационной безопасности.

***Тема 8. Анализ и оценка рисков информационной безопасности. Часть 1***

1. **<u>Лабораторная работа №6</u>. «Создание физической модели данных. Прямое и обратное проектирование».**

Создание физического уровня модели данных. Подуровни физического уровня модели данных. Выбор сервера. Таблицы, колонки и представления (view). Правила валидации и значения по умолчанию. Индексы. Триггеры и хранимые процедуры. Проектирование хранилищ данных. Вычисление размера базы данных. Преобразование моделей данных. Стандарты типов данных. Создание новой модели на основе существующей. Выгрузка физической модели данных из ERWin в SQL Server. Обратное проектирование и синхронизация моделей. Макрокоманды ERwin

**Задание**

Выполнить методические указания лабораторной работы № 3 лабораторного практикума по ERwin для создания физической модели данных ИС компании, специализирующейся на сборке и реализации компьютеров.

1. Создайте физическую модель данных SQL Server на основе ранее созданной логической. Переименуйте таблицы, поля.
2. Установите правила валидации и значения по умолчанию для атрибутов, установите автонумерацию для первичных ключей.

3. Создайте пользовательские типы данных Валюта, Номер телефона, Фамилия, Имя, Отчество, Адрес.
4. Создайте индексы
5. Создайте представления.
6. Создайте сценарии на уровне базы данных и отдельных таблиц для обеспечения целостности в ней и настройки прав пользователей для доступа к БД и ее элементам.
7. Сгенерируйте БД SQL Server и заполните ее с помощью прямого проектирования. Вставьте в БД новые таблицы. Осуществите обратное проектирование из SQL Server в ERWin в новую физическую модель.
8. Рассчитайте размер БД через 2 года после начала ее использования
9. Задайте стандарт типов данных для новой физической модели.

**Контрольные вопросы**

1. Подуровни физического уровня модели данных.
2. Назначение физической модели данных. Создание новой физической модели. Создание физической модели на основе существующих моделей.
3. Выбор сервера модели. Конвертация типов данных. Стандарт типов.
4. Таблицы, колонки и представления.
5. Правила валидации. Значение по умолчанию.
6. Индексы.
7. Триггеры, хранимые процедуры, скрипты “до и после генерации”.
8. Размерная модель. Различия реляционной и размерной модели. Роли таблиц в размерной модели.
9. Схемы размерных моделей: звезда и снежинка.
10. Свойства таблиц размерности: типы таблицы, правила хранения данных.
11. Вычисление размера базы данных.
12. Источники. Связка данных с источниками.
13. Прямое и обратное проектирование.
14. Синхронизация моделей.

### *2. Рейтинговая контрольная работа 6*

1. Инструментальная среда Process Modeler.
2. Принципы построения модели IDEF0.
3. Работы в IDEF0 (Activity).
4. Стрелки в IDEF0 (Arrow).
5. Нумерация работ и диаграмм.
6. Диаграммы дерева узлов и FEO.
7. Слияние и расщепление моделей.
8. Метод описания процессов IDEF3
9. Диаграммы
10. Единицы работ
11. Связи

## *Раздел 9. Анализ и оценка рисков информационной безопасности. Часть 2.*

**Лабораторная работа №7. «Объектно-ориентированный подход к проектированию ИС».**

Полиморфизм. Отличия от традиционных подходов. Визуальное моделирование. Определение. Основная цель ВМ. Объектно-ориентированный подходы к проектированию с использованием языка UML. Взаимосвязь нотации UML, методологии, инструментальных средств. Метод Буча, OMT и UML.

Классификация моделей в языке UML. Представления архитектуры ПО. Рекомендации по изображению диаграмм в нотации языка UML. Основные элементы языка UML. Механизмы расширения UML.

Диаграммы языка UML: диаграммы вариантов использования (Use Case Diagrams), диаграммы классов (Class Diagrams), диаграммы взаимодействия (последовательности и кооперации), диаграммы состояний, деятельности, компонентов и размещения.

Объектный язык ограничений (OCL). Понятие ограничения и его виды. Контекст OCL-выражения. Операции OCL. Обозначение навигаций в языке OCL. Виды коллекций и операции над ними. Характеристики OCL.

**Задание**

Выполнить методические указания с 1 по 7 лабораторного практикума по Rational Rose для создания проекта новой информационной системы университета взамен старой системы на мейнфрейме.

Новая система должна позволять студентам регистрироваться на курсы и просматривать свои табели успеваемости с персональных компьютеров, подключенных к локальной сети университета. Профессора должны иметь доступ к онлайновой системе, чтобы указать курсы, которые они будут читать, и проставить оценки за курсы.

Из-за недостатка средств университет не в состоянии заменить сразу всю существующую систему. По этой причине используется в прежнем виде база данных, содержащая всю информацию о курсах (каталог курсов). Эта база данных поддерживается реляционной СУБД. Новая система будет работать с существующей БД в режиме доступа, без обновления.

В начале каждого семестра студенты могут запросить каталог курсов, содержащий список курсов, предлагаемых в данном семестре. Информация о каждом курсе должна включать имя профессора, наименование кафедры и требования к предварительному уровню подготовки (прослушанным курсам).

Новая система должна позволять студентам выбирать четыре курса в предстоящем семестре. Дополнительно каждый студент может указать два альтернативных курса на тот случай, если какой-либо из выбранных им курсов окажется уже заполненным или отмененным.

На каждый курс может записаться не более десяти и не менее трех студентов (если менее трех, то курс будет отменен). В каждом семестре существует период времени, когда студенты могут изменить свои планы. В это время студенты должны иметь доступ к системе, чтобы добавить или удалить выбранные курсы. После того, как процесс регистрации некоторого студента завершен, система регистрации направляет информацию в расчетную систему, чтобы студент мог внести плату за семестр. Если курс окажется заполненным в процессе регистрации, студент должен быть извещен об этом до окончательного формирования его личного учебного плана.

В конце семестра студенты должны иметь доступ к системе для просмотра своих электронных табелей успеваемости. Поскольку эта информация конфиденциальная, система должна обеспечивать ее защиту от несанкционированного доступа.

Профессора должны иметь доступ к онлайновой системе, чтобы указать курсы, которые они будут читать, и просмотреть список студентов, записавшихся на их курсы. Кроме этого, профессора должны иметь возможность проставить оценки за курсы.

*Функциональные возможности*:

- система должна обеспечивать многопользовательский режим работы;
- если конкретный курс оказывается заполненным в то время, когда студент формирует свой учебный график, включающий данный курс, то система должна известить его об этом.

*Удобство использования*: пользовательский интерфейс должен быть совместимым с Windows.

*Надежность*: система должна быть в работоспособном состоянии 24 часа в день семь дней в неделю, время простоя – не более 10%.
*Производительность*: система должна поддерживать до 2000 одновременно работающих с центральной базой данных пользователей и до 500 пользователей, одновременно работающих с локальными серверами.
*Безопасность*:

- система не должна позволять студентам изменять любые учебные графики, кроме своих собственных, а также не должна позволять профессорам модифицировать конкретные курсы, выбранные другими профессорами;
- только профессора имеют право ставить студентам оценки;
- только регистратор может изменять любую информацию о студентах.

Проектные ограничения: система должна быть интегрирована с существующей системой каталога курсов, функционирующей на основе реляционной СУБД.

**Порядок выполнения лабораторных работ**

1. Создание действующих лиц и модели вариантов использования
2. Идентификация ключевых абстракций и анализ вариантов использования
3. Создание диаграмм последовательности.
4. Создание кооперативной диаграммы
5. Проектирование архитектуры системы
6. Проектирование баз данных
7. Реализация системы

**Контрольные вопросы**

1. Диаграммы вариантов использования и бизнес-вариантов использования.
2. Диаграмма классов и пакетов.
3. Диаграммы взаимодействия
4. Диаграммы состояний
5. Диаграммы деятельности
6. Диаграммы компонентов и размещения.

***2. Рейтинговая контрольная работа 7***

1. Стоимостный анализ (Activity Based Costing)
2. Свойства, определяемые пользователем (User Defined Properties)
3. Встроенные шаблоны отчетов
4. Создание отчетов с помощью Report Template Builder
5. Слияние и расщепление моделей
6. Копирование и перемещение работ с использованием навигатора
7. Модели AS-IS и TO-BE.
8. Диаграммы потоков данных (Data Flow Diagramming).
9. Работы в DFD.

### *Тема 10. Проектирование системы информационной безопасности*

#### *1. Учебный проект*

**Вариант 1.**

Разработать модель ИС по выбранной студентом теме. При разработке моделей использовать нотации IDEF0, DFD, IDEF3. Модель должна адекватно отображать задачу и соответствовать семантическим правилам нотаций. Для построения моделей использовать Microsoft Visio или любое свободно распространяемое CASE-средство (например, Dia).

**Порядок выполнения задания:**

1. Определить цель, точку зрения и область моделирования.
2. Собрать информацию по предметной области.
3. Построить модель IDEF0 для описания процессов в соответствии с собранной информацией.

4. Построить модель DFD для описания документооборота и обработки информации.
5. Построить модель IDEF3 для описания логики бизнес-процессов.

**Вариант 2.**
Разработать модель данных в нотации IDEF1X для выбранной студентом предметной области (предметная область предлагается студентом самостоятельно). Модель должна адекватно отображать задачу и соответствовать семантическим правилам нотаций. Для построения моделей использовать Microsoft Visio или любое свободно распространяемое CASE-средство.

**Порядок выполнения задания:**
1. Собрать и изучить информацию по предметной области.
2. Определить сущности для логического уровня модели данных.
3. Определить состав атрибутов для каждой сущности
4. Определить связи между сущностями
5. Построить логическую модель данных, включающую выделенные элементы
6. Проанализировать и, при необходимости, нормализовать структуру
7. Выбрать СУБД для реализации модели
8. Создать физическую модель данных на основе построенной ранее логической модели.

**Вариант 3.**
Установите соответствие между моделью данных и моделью процессов, созданных при выполнении предыдущих индивидуальных заданий

**Порядок выполнения задания:**
1. Выполните экспорт данных из модели данных в модель процессов
2. Создайте дополнительные сущности и атрибуты в модели процессов
3. Свяжите стрелки на диаграмме процессов с импортированными и созданными сущностями и атрибутами.
4. Задокументируйте воздействия работ на данные
5. Создайте отчет Data Usage Report в модели процессов
6. Экспортируйте данные из модели процессов в модель данных
7. Создайте отчет по сущностям с помощью Report Template Builder

**Вариант 4.**
Создайте физическую модель для модели данных логического уровня, созданной при выполнении индивидуального задания № 2

**Порядок выполнения задания:**
1. Создайте физическую модель данных SQL Server на основе ранее созданной логической. Переименуйте таблицы, поля.
2. Установите правила валидации, значения по умолчанию и пользовательские типы данных для атрибутов, установите автонумерацию для первичных ключей.
3. Создайте 1-2 представления для наиболее часто выполняемых запросов.
4. Создайте сценарии на уровне базы данных и отдельных таблиц для обеспечения целостности в ней и настройки прав пользователей для доступа к БД и ее элементам
5. Сгенерируйте БД SQL Server и заполните ее с помощью прямого проектирования. Вставьте в БД новые таблицы.
7. Осуществите обратное проектирование из SQL Server в новую физическую модель.
8. Рассчитайте размер БД через 2 года после начала ее использования
9. Задайте стандарт типов данных для новой физической модели.

***Тема 11. Эксплуатация и модификация системы информационной безопасности1.***
***1. Итоговое тестирование***
1. Состав Функциональной диаграммы:

a. *Блоки (действия) и дуги (вход, выход, управление, механизм),*
b. *Блоки (действия), внешние сущности и дуги (вход, выход, управление, механизм),*
c. *Блоки (действия) и потоки данных,*
d. *Внешние сущности и дуги (вход, выход, управление, механизм).*

2. Внешняя сущность на диаграмме потоков данных это:
   a. *Материальный объект или физическое лицо, представляющие собой источник или приемник информации,*
   b. *База данных,*
   c. *Абстрактное устройство для хранения информации,*
   d. *Внешняя Проект информационной системы по отношению к проектируемой системе.*
3. Базовыми понятиями диаграммы «сущность-связь» являются:
   a. *Внешние сущности и потоки данных,*
   b. *Внешние сущности и связь,*
   c. *Сущности, связь, и атрибут,*
   d. *Сущность и связь.*
4. Прецедентом (Use Case) называется:
   a. *Описание множества последовательностей действий выполняемых системой, чтобы актер мог получить определенный результат,*
   b. *Описание множества событий вне системы связанных с актером,*
   c. *Описание множества внешних сущностей,*
   d. *Описание множества потоков событий.*
5. Выберите правильную структуру класса:
   a. *Класс – подкласс – свойства,*
   b. *Имя – операции – результат,*
   c. *Группа – свойства – обязанности,*
   d. *Имя – атрибуты – операции.*
6. Базовыми отношениями на диаграмме классов являются:
   a. *Отношение зависимости,*
   b. *Отношение ассоциаций,*
   c. *Отношение обобщения,*
   d. *Отношение реализации.*
7. линия жизни объекта на диаграмме последовательности изображается в виде:
   a. *Вертикальной линий ассоциированной с объектом и с символом в виде латинской буквой X на конце,*
   b. *Горизонтальной линией ассоциированной с объектом,*
   c. *Вертикальной пунктирной линией ассоциированной с объектом,*
   d. *Горизонтальной пунктированной линией ассоциированной с объектом и с символом в виде латинской буквой X на конце.*
8. При распределении обязанностей классы должны быть:
   a. *Большие,*
   b. *Маленькие,*
   c. *Средние,*
   d. *В зависимости от системы.*
9. Чтобы показать отношение наследования («IS A») между классами используют:
   a. *Отношение обобщение,*
   b. *Отношение уточнение,*
   c. *Отношение зависимости,*
   d. *Нет правильного ответа.*
10. Отношение, в котором один из классов имеет более высокий ранг и состоит из нескольких меньших по рангу называется:

a. *Композицией,*
b. *Реализацией,*
c. *Обобщением,*
d. *Агрегированием,*
e. *Нет правильного ответа.*

11. Отношения, зависимости и обобщения в отличие от ассоциаций является:
    a. *Кратными,*
    b. *Односторонними,*
    c. *Двунаправленными,*
    d. *У них нет реализаций.*
12. Какие диаграммы используются при моделировании динамических аспектов системы:
    a. *Развертывания,*
    b. *Последовательности,*
    c. *Состояния,*
    d. *Прецедентов,*
    e. *Кооперации,*
    f. *Классов.*
13. На каких диаграммах не отображается отношение обобщения:
    a. *Диаграмма последовательности,*
    b. *Диаграмма сотрудничества,*
    c. *Диаграмма классов,*
    d. *Диаграмма прецедентов*.
14. В чем заключается суть статического моделирования:
    a. *В представлении структуры системы,*
    b. *В описании предметной области,*
    c. *Все выше проведенные пункты,*
    d. *Ни на один из вышеперечисленных пунктов.*
15. В чем заключается суть разбиения на классы:
    a. *В снижении сложности системы путем декомпозиции на составляющие элементы,*
    b. *В четком и не образующем разночтений представлении структуры системы,*
    c. *В четком и не образующем разночтений представлении поведения системы*
    d. *Все вышеперечисленные пункты,*
    e. *Ни один из вышеперечисленных пунктов.*
16. модель деятельности (или функциональная модель) рассматривает систему как:
    a. *Набор действий,*
    b. *Набор объектов,*
    c. *Набор классов,*
    d. *Набор данных.*
17. Дайте определение жизненного цикла программного обеспечения:
    a. *Определяется как период времени, который начинается с момента принятия решения с необходимости создания ПО и заканчивается в момент его полного изъятия из эксплуатации.*
    b. *Определяется как период времени, который начинается с момента принятия решения о необходимости создания ПО и заканчивается в момент его разработки.*
    c. *Определяется как период времени, который начинается с момента принятия решения о необходимости создания ПО и заканчивается в момент запуска его в эксплуатацию.*
18. Какие из перечисленных процессов входят в группу «Вспомогательные процессы ЖЦ ПО»:
    a. *Управление конфигурацией,*

b. *Обеспечение качества,*
c. *Верификация,*
d. *Аттестация,*
e. *Современная оценка,*
f. *Аудит,*
g. *Документирование,*
h. Все вышеперечисленные пункты.

19. основными компонентами диаграмм потоков данных являются (5 правильных ответов):
    a. *Внешние сущности,*
    b. *Классы и подклассы,*
    c. *Системы и подсистемы,*
    d. *Процессы,*
    e. *Объекты,*
    f. *Накопители данных,*
    g. *Потоки данных.*
20. Основным нормативным документом, регламентирующим состав процессов ЖЦ ПО, является:
    a. *Международный стандарт ISS/IEC 12207,*
    b. *Международный стандарт ISO/IEC 11307,*
    c. *Международный стандарт OSO/IEC 12207,*
    d. *Международный стандарт ISO/IEC 11207,*
21. Какие, применяемые к ассоциациям, дополнения существуют:
    a. *Направление,*
    b. *Роль,*
    c. *Агрегирование,*
    d. *Сущность,*
    e. *Имя,*
    f. *Кратность, все существуют.*
22. Атрибут на диаграмме «сущность-связь» может быть:
    a. *Ключевым либо уникальным,*
    b. *Уникальным либо обязательным,*
    c. *Уникальным либо необязательным,*
    d. *Обязательным либо необязательным.*
23. Любой прецедент должен иметь:
    a. *Имя,*
    b. *Уникальное имя внутри модели,*
    c. *Уникальное имя внутри пакета,*
    d. *Уникальный атрибут.*
24. Квантор видимости атрибута класса может принимать следующие значения:
    a. *Общедоступный,*
    b. *Закрытый,*
    c. *Защищенный,*
    d. *Секретный.*
25. графически отношение зависимости изображается:
    a. *Сплошной линией между соответствующими элементами,*
    b. *Сплошной линий между соответствующими элементами со стрелкой на одном из ее концов,*
    c. *Пунктирной линией между соответствующими элементами со стрелкой на одном из ее концов.*
    d. *Пунктирной линией между соответствующими элементами.*
26. Основная проблема спиральной модели ЖЦ ПО:

a. *Определение момента перехода на следующую стадию,*
b. *Формирование проектной документации,*
c. *Запаздывание с получением результатов,*
d. *Планирование затрат на разработку ПО.*

**Перечень вопросов к экзамену**

1. Виды автоматизированных систем и их характеристики
2. Виды обеспечения автоматизированных систем.
3. Автоматизированные системы управления предприятиями. Область применения и архитектура.
4. Автоматизированные системы управления технологическими процессами. Область применения и архитектура.
5. Ресурсы автоматизированных систем и основные требования к их защите.
6. Перечень и основные характеристики подсистем обеспечения информационной безопасности автоматизированной системы.
7. Основные положения РД Гостехкомиссии «Классификация автоматизированных систем и требования по защите информации».
8. Назначение и основные функции подсистемы управления доступом.
9. Организация доступа к ресурсам автоматизированной системы. Идентификация, аутентификация и авторизация.
10. Общая схема идентификации и аутентификации. Аутентификация с доверенной третьей стороной.
11. Модели разграничения доступа. Базовые представления. Модель состояний.
12. Дискреционное разграничение доступа.
13. Мандатное разграничение доступа.
14. Ролевое разграничение доступа.
15. Основные требования к криптографической подсистеме.
16. Принципы построения шифров. Классификация шифров.
17. Симметричная криптосистема шифрования. Основные понятия и схема применения.
18. Ассимметричная криптосистема шифрования. Основные понятия и схема применения.
19. Понятие цифровой подписи. Механизм формирования цифровой подписи.
20. Понятие функции хэширования. Применение Хэш-функций.
21. Основные требования к подсистеме обеспечения целостности,
22. Базовые методы резервного копирования и восстановления данных.
23. Основные требования к подсистеме защиты от вредоносных программ.
24. Компьютерные вирусы и программные закладки. Классификация компьютерных вирусов.
25. Классификация программных закладок. Классификация автоматизированных систем по уровню контроля недекларированных возможностей. Требования к уровням контроля.
26. Основные каналы распространения вредоносных программ.
27. Методы предупреждения вирусного заражения. Методы обезвреживания компьютерных вирусов.
28. Использование облачных технологий в антивирусном программном обеспечении.
29. Классификация возможных угроз информационным объектам автоматизированной системы.
30. Модель нарушителя. Классификация нарушителя. Основные определения и базовые понятия.
31. Каналы несанкционированного доступа к информации.

32. Угрозы безопасности ресурсам автоматизированной системы. Идентификация угроз. Причины появления угроз.

33. Классификация уязвимостей автоматизированных систем.

34. Классификация защищенности СВТ. Требования Руководящих документов Гостехкомиссии.

35. Классификация межсетевых экранов. Требования руководящих документрв Гостехкомиссии.

36. Цель разработки и структура Общих критериев ИБ.

37. Механизм описания требований к безопасности. Профиль защиты и задание по безопасности.

38. Структура профиля защиты по общим критериям.

39. Содержание задания по безопасности.

40. Жизненный цикл автоматизированной системы. Существующие подходы к проектированию автоматизированных систем.

41. Понятие встроенной и добавочной защиты. Требования и задачи, выполняемые системой добавочной защиты.

42. Результаты и стадии проектирования автоматизированных систем.

43. Организационное обеспечение автоматизированных систем. Состав и требования к содержанию организационно-распорядительной документации.

44. Понятие политики информационной безопасности. Обязательные разделы политики безопасности.

45. Понятие инцидента ИБ. Понятие информационного актива. Реализация угрозы ИБ. Понятие уязвимости.

46. Процесс оценки рисков ИБ. Основные этапы оценки рисков ИБ.

47. Требования к оценке рисков ИБ. Результаты оценки рисков ИБ.

48. Идентификация и классификация уязвимостей. Качественная и количественная оценка рисков ИБ.

49. Определение ценности активов автоматизированных систем. Применение опросных листов и экспертных оценок.

50. Детальная оценка рисков информационной безопасности. Основные нормативные документы по управлению рисками информационной безопасности.

**Таблица 9 – Примеры оценочных средств с ключами правильных ответов**

| № п/п | Тип задания | Формулировка задания | Правильный ответ | Время выполнения (в минутах) |
|---|---|---|---|---|
| ПК-2 – способен выполнять работы по установке, настройке и техническом у обслуживанию защищенных технических средств обработки информации | | | | |
| 1. | Задание закрытого типа | Для описания функциональных требований к информационной системе используется:<br>1) Диаграмма деятельности,<br>2) Диаграмма последовательности,<br>3) Диаграмма вариантов использования. | 3 | 1 |
| 2. | | Функциональные требования к информационной системе описываются с помощью:<br>1) Прецедентов, | 1 | 1 |

| № п/п | Тип задания | Формулировка задания | Правильный ответ | Время выполнения (в минутах) |
|---|---|---|---|---|
| | | 2) Классов,<br>3) Отношений включения,<br>4) Управлений на диаграмме IDEF0. | | |
| 3. | | Разработка функциональных моделей организаций (моделей «как есть» и «как должно быть») позволяет:<br>1) Глубоко изучить природу бизнес-процессов<br>2) Выявить ключевые бизнес-процессы относительно целей организации Провести реструктуризацию (реинжиниринг) старых и разработку новых процессов,<br>3) Описать структуру базы данных организации. | 1<br>2 | 1 |
| 4. | | Накопители данных на диаграмме потоков данных проекта ИС это:<br>1) Абстрактное устройство для хранения информации,<br>2) База данных,<br>3) Таблица в базе данных,<br>Магнитный носитель. | 1 | 1 |
| 5. | | Внешняя сущность на диаграмме потоков данных проекта ИС это:<br>1) Материальный объект или физическое лицо, представляющие собой источник или приемник информации,<br>2) База данных,<br>3) Абстрактное устройство для хранения информации,<br>4) Внешняя Проект информационной системы по отношению к проектируемой системе. | 1 | 1 |
| 6. | Задание открытого типа | Охарактеризуйте стадии и этапы жизненного цикла информационных систем | Стадии жизненного цикла – отражают состояния ИС и их изменения. Этапы | 3 |

| № п/п | Тип задания | Формулировка задания | Правильный ответ | Время выполнения (в минутах) |
|---|---|---|---|---|
| | | | жизненного цикла – входят в состав стадий; предполагают выполнение определенного объема работ в течение ограниченного времени. | |
| 7. | | Охарактеризуйте процессы жизненного цикла информационных систем | Процессы жизненного цикла могут применяться любой организацией при приобретении и использовании или создании и поставке системы. Процессы жизненного цикла распространяются на любой уровень системной иерархии и на любую стадию жизненного цикла. Процессы жизненного цикла основываются на принципах модульности (максимальная слаженность функций процесса и минимальная связь между процессами) и собственности (процесс связывается с ответственностью) | 4 |
| 8. | | Опишите особенности каскадной модели жизненного цикла информационных систем | Переход на следующий этап осуществляется после полного окончания работ по предыдущему этапу, при этом оформляется полный комплект рабочей документации. Все этапы выполняются в строгой последовательности с | 5 |

| № п/п | Тип задания | Формулировка задания | Правильный ответ | Время выполнения (в минутах) |
|---|---|---|---|---|
| | | | утвержденными сроками и четкими затратами. Применялась в условиях полной определенности решаемых задач и совершенно не приемлема когда и разработчики и заказчики не имеют четкого видения всех особенностей проектируемой ИС. Отсутствует гибкость в работе над созданием ИС | |
| 9. | | Опишите особенности спиральная модель жизненного цикла ИС | Происходит ориентация на модернизацию информационной системы. Осуществляется аккумулирование всех решений в процессе проектирования и создания моделей и прототипов информационной системы. Проводится анализ издержек и всех рисков в процессе проектирования ИС. | 5 |
| 10. | | Опишите в чем сущность структурного подхода к проектированию ИС. | Сущность структурного подхода к разработке ИС заключается в ее декомпозиции (разбиении) на автоматизируемые функции. Система разбивается на функциональные подсистемы, которые в свою очередь делятся | 5 |

| № п/п | Тип задания | Формулировка задания | Правильный ответ | Время выполнения (в минутах) |
|---|---|---|---|---|
| | | | на подфункции, подразделяемые на задачи и так далее. | |
| ПК-4 – способен осуществлять внедрение систем защиты информации для обеспечения информационной безопасности автоматизированных систем | | | | |
| 1. | Задание закрытого типа | Основная проблема спиральной модели ЖЦ ПО:<br>1) Определение момента перехода на следующую стадию,<br>2) Формирование проектной документации,<br>3) Запаздывание с получением результатов,<br>4) Планирование затрат на разработку ПО. | 1 | 1 |
| 2. | | Для документирования функциональных требований к ИС используется:<br>1) Диаграмма вариантов использования,<br>2) Диаграмма сущность-связь,<br>3) Диаграмма классов,<br>4) Диаграмма жизненного цикла ИС. | 1 | 1 |
| 3. | | Какие из перечисленных процессов входят в группу «Организационные процессы ЖЦ ПО»<br>1) Управление,<br>2) Обеспечение качества,<br>3) Поставка,<br>4) Аттестация,<br>5) Усовершенствование,<br>6) Создание инфраструктуры,<br>7) Документирование,<br>8) Сопровождение,<br>9) Все выше перечисленные. | 1<br>5<br>6 | 1 |
| 4. | | Какие из перечисленных процессов входят в группу «Основные процессы ЖЦ ПО»<br>1) Управление,<br>2) Обеспечение качества,<br>3) Поставка,<br>4) Аттестация, | 3<br>8 | 1 |

| № п/п | Тип задания | Формулировка задания | Правильный ответ | Время выполнения (в минутах) |
|---|---|---|---|---|
| | | 5) Усовершенствование,<br>6) Создание инфраструктуры,<br>7) Документирование,<br>8) Сопровождение,<br>9) Все выше перечисленные. | | |
| 5. | | Какие из перечисленных процессов входят в группу «Вспомогательные процессы ЖЦ ПО»<br>1) Управление конфигурацией,<br>2) Обеспечение качества,<br>3) Поставка,<br>4) Аттестация,<br>5) Усовершенствование,<br>6) Создание инфраструктуры,<br>7) Документирование,<br>8) Сопровождение,<br>9) Все выше перечисленные. | 2<br>4<br>7 | 1 |
| 6. | Задание открытого типа | Перечислите этапы SADT | Сбор информации и анализ информации о предметной области. Документирование полученной информации. Моделирование (IDEF0). Корректура модели в процессе итеративного рецензирования | 5 |
| 7. | | Перечислите элементы UML | Синтаксис, то есть определение правил построения конструкций языка. Семантика, то есть определение правил, в соответствии с которыми конструкции языка приобретают смысловое значение. Прагматика, то есть определение правил использования конструкций языка для достижения нужных нам целей. | 5 |

| № п/п | Тип задания | Формулировка задания | Правильный ответ | Время выполнения (в минутах) |
|---|---|---|---|---|
| 8. | | Какие графические нотации рассматриваются в рамках структурного подхода | Диаграммы "сущность-связь" (Entity-Relationship Diagrams, ERD). Диаграммы функционального моделирования (Structured Analysis and Design Technique, SADT). Диаграммы потоков данных (Data Flow Diagrams, DFD). | 5 |
| 9. | | Перечислите основные требования к языку моделирования | Язык моделирования должен позволять моделировать не только программное обеспечение, но и более широкие классы систем и бизнес-приложений, с использованием объектно-ориентированных понятий. Язык моделирования должен явным образом обеспечивать взаимосвязь между базовыми понятиями для моделей концептуального и физического уровней. А также обеспечивать масштабируемость моделей, что является важной особенностью сложных многоцелевых систем. Должен быть понятен аналитикам и программистам, а также должен поддерживаться специальными инструментальными средствами, | 5 |

| № п/п | Тип задания | Формулировка задания | Правильный ответ | Время выполнения (в минутах) |
|---|---|---|---|---|
| | | | реализованными на различных компьютерных платформах. | |
| 10. | | Охарактеризуйте UML как средство проектирования | UML позволяет строить модели программных систем , по которым может производиться генерация каркасного кода проектируемых приложений. "Реверс-инжиниринг" - создание UML-модели из существующего кода приложения | 5 |

Полный комплект оценочных материалов по дисциплине (модулю) (фонд оценочных средств) хранится в электронном виде на кафедре, утверждающей рабочую программу дисциплины (модуля), и в Центре мониторинга и аудита качества обучения.

**7.4. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине (модулю)**

Методические рекомендации по выполнению лабораторных работ, проведению зачета и экзамена

Критерии оценки обсуждения вопросов по теме:

– оценка «отлично» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы;

– оценка «хорошо» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы, допущены некоторые неточности, имеется одна негрубая ошибка.

– оценка «удовлетворительно» выставляется обучающемуся, если студент ответил на вопросы преимущественно верно, имеются затруднения в формулировке выводов, имеются одна или две негрубые ошибки;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не дал ответы на поставленные вопросы, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки.

Отчет по лабораторной работе

Отчет по лабораторной работе представляется в электронном виде. Защита отчета проходит в форме доклада студента по выполненной работе и ответов на вопросы преподавателя. В случае, если оформление отчета и поведение студента во время защиты соответствуют указанным требованиям, студент получает максимальное количество баллов.

Основаниями для снижения количества баллов в диапазоне от max до min являются:

- отсутствие списка использованной литературы,

- небрежное выполнение,
- отсутствие выводов.

Отчет не может быть принят и подлежит доработке в случае:
- отсутствия необходимых разделов,
- отсутствия необходимого графического материала,
- неверных результатов расчета.

В отчете по выполненной лабораторной работе должны быть указаны:
- тема лабораторной работы,
- пакет документов в соответствии с темой лабораторной работы,
- использованная литература.

Критерии оценки по практическим работам:

– оценка «отлично» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы и учел основные нормативно-правовые документы по информационной безопасности;

– оценка «хорошо» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы и учел основные нормативно-правовые документы по информационной безопасности, допущены некоторые неточности, имеется одна негрубая ошибка.

– оценка «удовлетворительно» выставляется обучающемуся, если студент ответил на вопросы преимущественно верно, имеются затруднения в формулировке выводов, имеются одна или две негрубые ошибки, учтены не все нормативно-правовые документы по информационной безопасности;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не дал ответы на поставленные вопросы, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки, отсутствуют знания нормативно-правовых документов по информационной безопасности.

Контрольные работы

Контрольная работа состоит из 2-х заданий.

Основаниями для снижения оценки за задание являются:
- ошибки в объяснениях и комментариях при верно выполненном задании;
- неполный ответ для теоретический заданий;
- небрежное выполнение;
- многократное переписывание контрольной работы.

Задание не может быть засчитано, если:
- даны два неверных ответа на теоретические вопросы.

Критерии оценки контрольных работ:

– оценка «отлично» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы и учел основные нормативно-правовые документы по информационной безопасности;

– оценка «хорошо» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы и учел основные нормативно-правовые документы по информационной безопасности, допущены некоторые неточности, имеется одна негрубая ошибка.

– оценка «удовлетворительно» выставляется обучающемуся, если студент ответил на вопросы преимущественно верно, имеются затруднения в формулировке выводов, имеются одна или две негрубые ошибки, учтены не все нормативно-правовые документы по информационной безопасности;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не дал ответы на поставленные вопросы, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки, отсутствуют знания нормативно-правовых документов по информационной безопасности.

Критерии оценки теста:

- оценка «отлично» выставляется студенту, если он умеет безошибочно самостоятельно обрабатывать и интерпретировать данные при решении задач, как в стандартной, так и в нестандартной формулировке;
- оценка «хорошо» выставляется студенту, если он умеет безошибочно самостоятельно обрабатывать и интерпретировать данные при решении задач в стандартной ситуации или за верное решение 75% - 89% заданий теста;
- оценка «удовлетворительно» выставляется студенту, если он умеет при решении задач обрабатывать данные с опорой на справочные материалы и помощь преподавателя, верно выполняя при этом 60% - 74% работы.
- оценка «неудовлетворительно» выставляется студенту, если он не умеет правильно обрабатывать данные, выполнил менее 60% заданий теста.
- оценка «зачтено» выставляется студенту, если тест студента оценен не ниже чем «удовлетворительно»;
- оценка «не зачтено», если тест оценен ниже чем «удовлетворительно».

Зачет

Оценивание студентов на зачете осуществляется в соответствие с требованиями и критериями 100-балльной шкалы. Учитываются как результаты текущего контроля, так и знания, навыки и умения, непосредственно показанные студентами в ходе зачета.

Экзамен

Экзамен заключается в письменном ответе на 2 теоретических вопроса и устном собеседовании по каждому теоретическому вопросу.

Основаниями для снижения оценки за теоретический вопрос являются:

- небрежное выполнение;
- неполный ответ;
- наличие мелких неточностей или незначительных искажений фактов;
- неточные объяснения при собеседовании;
- отсутствие ответов на заданные при собеседовании вопросы.

В соответствии с балльно-рейтинговой системой БАРС по дисциплине на экзамен во втором семестре отводится 100 баллов (40 баллов на текущие формы контроля, 10 баллов на бонусы и 50 баллов отводится на экзамен),

Оценивание студентов на экзамене осуществляется в соответствие с требованиями и критериями 100-балльной шкалы. Учитываются как результаты текущего контроля, так и знания, навыки и умения, непосредственно показанные студентами в ходе экзамена.

Критерии оценок на экзамене:

40-50 баллов – студент глубоко понимает пройденный материал, отвечает четко и всесторонне, умеет оценивать факты, самостоятельно рассуждает, отличается способностью обосновать выводы и разъяснять их в логической последовательности.

35-39 баллов – студент глубоко понимает пройденный материал, отвечает четко и всесторонне, умеет оценивать факты, самостоятельно рассуждает, отличается способностью обосновать выводы и разъяснять их в логической последовательности, но допускает отдельные неточности.

25-34 балла – студент глубоко понимает пройденный материал, отвечает четко и всесторонне, умеет оценивать факты, самостоятельно рассуждает, отличается способностью обосновать выводы и разъяснять их в логической последовательности, но допускает некоторые ошибки общего характера.

20-22 балла – студент хорошо понимает пройденный материал, но не может теоретически обосновать некоторые выводы.

15-19 баллов – студент отвечает в основном правильно, но чувствуется механическое заучивание материала.

11-14 баллов – в ответе студента имеются существенные недостатки, материал охвачен «половинчато», в рассуждениях допускаются ошибки.

10 баллов – ответ студента правилен лишь частично, при разъяснении материала допускаются серьезные ошибки.

6-9 баллов – студент имеет общее представление о теме, но не умеет логически обосновать свои мысли.

1-5 баллов – студент имеет лишь частичное представление о теме. 0 баллов – нет ответа.

**Таблица 10 – Технологическая карта рейтинговых баллов по дисциплине (модулю) (7 семестр)**

| № п/п | Контролируемые мероприятия | Количество мероприятий / баллы | Максимальное количество баллов | Срок представления |
|---|---|---|---|---|
| **Основной блок** | | | | |
| 1. | *Ответ на занятии* | 16/2 | 32 | В соответствии с таблицей 2 |
| 2. | *Выполнение лабораторных работ* | 4/7 | 28 | |
| 3. | *Выполнение контрольных работ* | 4/5 | 20 | |
| 4. | *Тест* | 2/5 | 10 | |
| **Всего** | | | **90** | - |
| **Блок бонусов** | | | | |
| 5. | *Посещение занятий без пропусков* | | 3 | |
| 6. | *Своевременное выполнение всех заданий* | | 3 | |
| 7. | *Активность студента на занятии* | | 4 | |
| **Всего** | | | **10** | - |
| **ИТОГО** | | | **100** | - |

**Таблица 10а – Технологическая карта рейтинговых баллов по дисциплине (модулю) (8 семестр)**

| № п/п | Контролируемые мероприятия | Количество мероприятий / баллы | Максимальное количество баллов | Срок представления |
|---|---|---|---|---|
| **Основной блок** | | | | |
| 1. | *Ответ на занятии* | 18/1 | 18 | В соответствии с таблицей 2 |
| 2. | *Выполнение лабораторных работ* | 3/2 | 6 | |
| 3. | *Выполнение контрольных работ* | 3/2 | 6 | |
| 4. | *Тест* | 1/5 | 5 | |
| 5. | *Учебный проект* | 1/5 | 5 | |
| **Всего** | | | **40** | - |
| **Блок бонусов** | | | | |
| 6. | *Посещение занятий без пропусков* | | 3 | |
| 7. | *Своевременное выполнение всех заданий* | | 3 | |
| 8. | *Активность студента на занятии* | | 4 | |
| **Всего** | | | **10** | - |
| **Дополнительный блок** | | | | |
| 9. | *Экзамен* | | 50 | |
| **Всего** | | | **50** | - |
| **ИТОГО** | | | **100** | - |

**Таблица 11 – Система штрафов (для одного занятия)**

| Показатель | Балл |
|---|---|
| *Опоздание на занятие* | - 1 |
| *Нарушение учебной дисциплины* | - 1 |
| *Неготовность к занятию* | - 2 |
| *Пропуск занятия без уважительной причины* | - 2 |

**Таблица 12 – Шкала перевода рейтинговых баллов в итоговую оценку за семестр по дисциплине (модулю)**

| Сумма баллов | Оценка по 4-балльной шкале | |
|---|---|---|
| 90–100 | 5 (отлично) | |
| 85–89 | 4 (хорошо) | |
| 75–84 | | |
| 70–74 | | |
| 65–69 | 3 (удовлетворительно) | |
| 60–64 | | |
| Ниже 60 | 2 (неудовлетворительно) | |

При реализации дисциплины (модуля) в зависимости от уровня подготовленности обучающихся могут быть использованы иные формы, методы контроля и оценочные средства, исходя из конкретной ситуации.

## 8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

### 8.1. Основная литература


1. Проектирование автоматизированных систем обработки информации и управления (АСОИУ): учебник / Я.А. Хетагуров. - М. : БИНОМ, 2015. - (Учебник для высшей школы). - URL: http://www.studentlibrary.ru/book/ISBN9785996329007.html (ЭБС «Консультант студента»).
2. Обнаружение вторжений в компьютерные сети (сетевые аномалии) : Учебное пособие для вузов / Под ред. профессора О.И. Шелухина. - М. : Горячая линия - Телеком, 2013. - URL: http://www.studentlibrary.ru/book/ISBN9785991203234.html (ЭБС «Консультант студента»).
3. Проектирование компонентов автоматизированных систем в примерах: учебное пособие / Волкова Т.В. - Оренбург: ОГУ, 2017. - URL: http://www.studentlibrary.ru/book/ISBN9785741017845.html (ЭБС «Консультант студента»).
4. Информационная безопасность открытых систем [/ Мельников Д.А. - М. : ФЛИНТА, 2014. - URL: http://www.studentlibrary.ru/book/ISBN9785976516137.html (ЭБС «Консультант студента»).
5. Автоматизация проектирования комплексных систем защиты информации / Аверченков В.И. - М. : ФЛИНТА, 2017. - URL: http://www.studentlibrary.ru/book/ISBN9785976529458.html (ЭБС «Консультант студента»).


### 8.2. Дополнительная литература


1. Проектирование информационных систем и баз данных: учеб. пособие / Стасышин В.М. - Новосибирск : Изд-во НГТУ, 2012. - URL: http://www.studentlibrary.ru/book/ISBN9785778221215.html (ЭБС «Консультант студента»).
2. Эксплуатация автоматизированных систем обработки информации и управления: метод. указания к выполнению лабораторных работ / В.М. Постников, С.Б. Спиридонов. - М. : Издательство МГТУ им. Н. Э. Баумана, 2012. - URL: http://www.studentlibrary.ru/book/bauman_0458.html (ЭБС «Консультант студента»).
3. Надежность и диагностика автоматизированных систем: Курс лекций / Васильев Р.Р., Салихов М.З. - М. : МИСиС, 2005. - URL: http://www.studentlibrary.ru/book/2227-8397-2005-06.html (ЭБС «Консультант студента»).
4. Проектирование автоматизированных систем производства [Электронный ресурс] : Учеб. пособие / В.Л. Конюх. - М. : Абрис, 2012. - URL: http://www.studentlibrary.ru/book/ISBN9785437200407.html (ЭБС «Консультант студента»).
5. Технология проектирования автоматизированных систем обработки информации и управления: Учебное пособие для вузов / Рудинский И.Д. - М. : Горячая линия - Телеком, 2011. - URL: http://www.studentlibrary.ru/book/ISBN9785991201483.html (ЭБС «Консультант студента»).
6. Безопасность информации в автоматизированных системах / В.В. Мельников. - М. : Финансы и статистика, 2003. - URL: http://www.studentlibrary.ru/book/ISBN5279025607.html (ЭБС «Консультант студента»).
7. Защита компьютерной информации. Эффективные методы и средства / Шаньгин В.Ф. - М. : ДМК Пресс, 2010. - URL: http://www.studentlibrary.ru/book/ISBN9785940745181.html (ЭБС «Консультант студента»).
8. Галатенко В.А. Основы информационной безопасности: курс лекций, учебное пособие. – Москва: ИНТУИТРУ «Интернет-университет Информационных Технологий», 2004. – 264 с. (45 экз.)
9. Голицына О.Л., Максимов Н.В., Попов И.И. Информационные системы: учебное пособие. М.: Форум. 2009. – 496 с. (40 экз.)

10. Мельников, В.П. Информационная безопасность и защита информации : доп. УМО по ун-тскому политех. образованию в качестве учеб. пособия для студентов вузов, обучающихся по специальности 230201 "Информационные системы и технологии" / В. П. Мельников, Клейменов, С.А., Петраков, А.М. ; под ред. С.А. Клейменова. - 4-изд. ; стер. - М. : Академия, 2009. - 336 с. - (Высшее профессиональное образование). - ISBN 978-5-7695-6150-4 : 306-46. (19 экз.)

### 8.3. Интернет-ресурсы, необходимые для освоения дисциплины (модуля)

1. **Электронно-библиотечная система (ЭБС) ООО «Политехресурс» «Консультант студента».** Многопрофильный образовательный ресурс «Консультант студента» является электронной библиотечной системой, предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Каталог в настоящее время содержит около 15000 наименований. www.studentlibrary.ru.

## 9. Материально-техническое обеспечение дисциплины

Для проведения лабораторных занятий необходима компьютерная аудитория, в которой организован доступ к сети Интернет и установлено программное обеспечение. Для проведения публичной защиты проектов, необходима мультимедийная аудитория с проектором.

Учебные аудитории, библиотеки АГУ, центр мониторинга и аудита качества образования, компьютерные классы, мультимедийные аудитории.

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. Для инвалидов содержание рабочей программы дисциплины (модуля) может определяться также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

## 10. ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ (МОДУЛЯ) ПРИ ОБУЧЕНИИ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а

требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т. д.). Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т. д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).