**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**
**ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ**
**имени академика М.Д. Миллионщикова**

«УТВЕРЖДАЮ»
Первый проректор-
проректор по ОД
И.Г. Гайрабеков
«26» 06 2026г.

# РАБОЧАЯ ПРОГРАММА

дисциплины

# «ПРОЕКТИРОВАНИЕ И ЭКСПЛУАТАЦИЯ ЗАЩИЩЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ»

**Направление подготовки**

10.03.01 *«Информационная безопасность»*

**Направленность (профиль)**

«*Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)*»

**Квалификация**

бакалавр

Год начала подготовки – 2026

Грозный – 2026

## 1. Цели и задачи дисциплины

**Целью дисциплины** «Проектирование и эксплуатация защищенных информационных систем» является, формирование компетентности в области проектирования и эксплуатации автоматизированных систем в защищенном исполнении, отдельных компонентов автоматизированных систем, с учетом требований нормативно-технической и методической документации по обеспечению безопасности информации. Теоретическая и практическая подготовка к деятельности, связанной с проектированием и эксплуатации защищенных автоматизированных информационных систем в своей профессиональной деятельности.

**Задачи дисциплины** «Проектирование и эксплуатация защищенных информационных систем»: освоение методологии, анализа и выбора принципов и методов проектирования и эксплуатации безопасных информационных систем.

## 2. Место дисциплины в структуре образовательной программы

Дисциплина «Проектирование и эксплуатация защищенных информационных систем» относится к формируемой участниками образовательных отношений части цикла ОП направления подготовки бакалавров 10.03.01 «Информационная безопасность» и изучается в 7 и 8 семестрах. Для изучения курса не требуется специальных знаний. В свою очередь, данный курс, помимо самостоятельного значения, является предшествующей дисциплиной для курса:

- Защита информационных процессов в компьютерных системах,
- Проектирование и эксплуатация защищенных информационных систем,
- Комплексное обеспечение защиты информации объекта информатизации.

## 3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

**Таблица 1**

| **Код по ОП** | **Индикаторы достижения** | **Планируемые результаты обучения по дисциплине (ЗУВ)** |
|---|---|---|
| **Общепрофессиональные** | | |

| | | |
|---|---|---|
| **ОПК-6**<br>Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю | **ОПК-6.1.** Знает основные нормативные правовые акты, нормативные и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.<br>**ОПК-6.2.** Умеет организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.<br>**ОПК-6.3.** Владеет навыками работы с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. | **Знать:** основные нормативные правовые акты, нормативные и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.<br>**Уметь:** организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.<br>**Владеть:** инструментарием, обеспечивающим программно-аппаратную защиту информационных ресурсов от изучения, модификации и копирования; навыками работы с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. |
| **ОПК-12**<br>Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования | **ОПК-12.1.** Знает основные исходные данные для проектирования подсистем.<br>**ОПК-12.2.** Умеет проводить экспериментальные исследования и проектировать подсистемы и средств обеспечения защиты информации.<br>**ОПК-12.3.** Владеет методами технико-экономического обоснования | **Знать:** основные исходные данные для проектирования подсистем.<br>**Уметь:** проводить экспериментальные исследования и проектировать подсистемы и средств обеспечения защиты информации.<br>**Владеть:** методами технико-экономического обоснования |

| | | |
|---|---|---|
| соответствующих проектных решений | соответствующих проектных решений. | соответствующих проектных решений. |
| **Профессиональные** | | |
| ПК-1. Способен управлять защитой информации в автоматизированных системах | **ПК-1.1.** Знает основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; методы защиты информации от несанкционированного доступа и утечки по техническим каналам; нормативные правовые акты в области защиты информации<br>**ПК-1.2.** Умеет определять подлежащие защите информационные ресурсы автоматизированных систем; оценивать информационные риски в автоматизированных системах; классифицировать и оценивать угрозы безопасности информации;<br>**ПК-1.3.** Владеет методикой оценки последствий выявленных инцидентов и обнаружения нарушения правил разграничения доступа | **Знать:** основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; методы защиты информации от несанкционированного доступа и утечки по техническим каналам; нормативные правовые акты в области защиты информации<br>**Уметь:** определять подлежащие защите информационные ресурсы автоматизированных систем; оценивать информационные риски в автоматизированных системах; классифицировать и оценивать угрозы безопасности информации;<br>**Владеть:** методикой оценки последствий выявленных инцидентов и обнаружения нарушения правил разграничения доступа |
| ПК-2. Способен выполнять работы по установке, настройке и техническому обслуживанию защищенных технических средств обработки информации | **ПК 2.1.** Знает 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 | **Знать:** ехнические 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<br>**Уметь:** проводить настройку |

| | | |
|---|---|---|
| | соответствие требованиям безопасности информации<br>**ПК 2.2.** Умеет 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.<br>**ПК 2.3.** Владеет методами защиты информации от несанкционированного доступа и специальных программных воздействий на нее | 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.<br>**Владеть:** методами защиты информации от несанкционированного доступа и специальных программных воздействий на нее |

**4. Объем дисциплины и виды учебной работы**

**Таблица 2**

| **Вид учебной работы** | **Всего часов/ зач.ед.** | | **Семестры** | | | |
|---|---|---|---|---|---|---|
| | | | **7** | **7** | **8** | **8** |
| | **ОФО** | **ОЗФО** | **ОФО** | **ОЗФО** | **ОФО** | **ОЗФО** |
| **Контактная работа (всего)** | **116/3,2** | **115/3,2** | **68/1,8** | **51/1,4** | **48/1,3** | **64/1,8** |
| В том числе: | | | | | | |
| Лекции | 58/1,6 | 49/1,4 | 34/0,9 | 17/0,5 | 24/0,6 | 32/0,9 |
| Практические занятия | | | | | | |
| Семинары | | | | | | |
| Лабораторные работы | 58/1,6 | 66/1,8 | 34/0,9 | 34/0,9 | 24/0,6 | 32/0,9 |
| **Самостоятельная работа (всего)** | **232/6,4** | **209/6,8** | **112/3,1** | **129/3,6** | **120/3,2** | **80/2,2** |
| В том числе: | | | | | | |
| Курсовая работа (проект) | 23/0,6 | 16/0,4 | - | - | 23/0,6 | 16/0,4 |
| ИТР | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Рефераты | | 23/0,6 | 29/0,9 | 23/0,6 | 29/0,9 | - | - |
| Работа над проектом | | 46/1,2 | 44/1,3 | 23/0,6 | 28/0,9 | 23/0,6 | 16/0,4 |
| *И(или) другие виды самостоятельной работы:* | | | | | | | |
| Подготовка к лабораторным работам | | 68/1,8 | 52/1,4 | 30/0,8 | 36/1 | 38/1,1 | 16/0,4 |
| Подготовка к практическим работам | | | | | | | |
| Подготовка к зачету | | 36/1 | 36/1 | 36/1 | 36/1 | - | - |
| Подготовка к экзамену | | 36/1 | 32/0,9 | - | - | 36/1 | 32/0,9 |
| **Контроль** | | **12/0,3** | **36/1** | | | **12/0,3** | **36/1** |
| **Вид отчетности** | | | | зачет | зачет | экзамен | экзамен |
| **Общая трудоемкость дисциплины** | **Всего в часах** | **360** | **360** | **180** | **180** | **180** | **180** |
| | **Всего в зач. единицах** | **10** | **10** | **5/2** | **5/2** | **5/2** | **5/2** |

**5. Содержание дисциплины**

**5.1. Разделы дисциплины и виды занятий**

**Таблица 3**

| № п/п | Наименование раздела дисциплины | Лекц. зан. часы | | Лаб.зан. часы | | Всего часов | |
|---|---|---|---|---|---|---|---|
| | | ОФО | ОЗФО | ОФО | ОЗФО | ОФО | ОЗФО |
| **7 семестр** | | | | | | | |
| 1 | Общие положения проектирования безопасных информационных систем. | 4 | 2 | 4 | 4 | 8 | 6 |
| 2 | Формирование требований к системе защиты информации информационной системы. | 10 | 5 | 10 | 10 | 20 | 15 |
| 3 | Разработка системы защиты информации информационной системы. | 10 | 5 | 10 | 10 | 20 | 15 |
| 4 | Реализация системы защиты информации в информационной системе. | 10 | 5 | 10 | 10 | 20 | 15 |
| **8 семестр** | | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 5 | Аттестация информационной системы на соответствие требованиям о защите информации и ввод ее в действие. | 10 | 12 | 10 | 12 | 20 | 24 |
| 6 | Эксплуатация системы защиты информации информационной системы. | 7 | 10 | 7 | 10 | 14 | 20 |
| 7 | Защита информации в ходе снятия с эксплуатации информационной системы. | 7 | 10 | 7 | 10 | 14 | 20 |

**5.2. Лекционные занятия**

**Таблица 4**

| № п/п | Наименование раздела дисциплины | Содержание раздела |
|---|---|---|
| **7 семестр** | | |
| 1. | Общие положения проектирования безопасных информационных систем. | Основы методологии проектирования информационных систем. Модели жизненного цикла. Методологии и технологии проектирования ИС. |
| 2. | Формирование требований к системе защиты информации информационной системы. | Определение актуальных угроз безопасности информации и разработка на их основе модели угроз. Классификация информационной системы. Цель и задачи обеспечения защиты информации в информационной системе. Перечень нормативных правовых актов, методических документов и национальных стандартов, требованиям которых должна соответствовать информационная система. Перечень типов объектов защиты информационной системы. Требования к мерам и средствам защиты информации, применяемым в информационной системе |
| 3. | Разработка системы защиты информации информационной системы. | Определение субъектов доступа (пользователи, процессы и иные субъекты доступа) и объектов доступа (устройства, объекты файловой системы, запускаемые и исполняемые модули, объекты системы управления базами данных, объекты, создаваемые прикладным программным обеспечением, иные объекты доступа). Состав мер по защите информации, обеспечивающих блокирование (нейтрализацию) актуальных угроз безопасности информации, и их содержание в соответствии с установленным классом защищенности информационной системы. Организационные меры, |

| | | |
|---|---|---|
| | | виды и типы средств защиты информации. компиляторов, загрузчиков, сборщиков Написание исходного кода компиляторов, загрузчиков, сборщиков Отладка компиляторов, загрузчиков, сборщиков Реинжиниринг разработанных компиляторов, загрузчиков, сборщиков, драйвера устройства 7 Логическая структура, состав (количество) и места размещения элементов системы защиты информации информационной системы. Выбор сертифицированных средств защиты информации с учетом их совместимости с информационными технологиями и техническими средствами обработки информации, функций безопасности этих средств и особенностей их реализации, а также класса защищенности информационной системы. Параметры настройки средств защиты информации, обеспечивающие реализацию мер по защите информации и блокирование (нейтрализацию) актуальных угроз безопасности информации, в том числе путем устранения возможных уязвимостей информационной системы. Эксплуатационная документация на систему защиты информации информационной системы. Тестирование системы защиты информации информационной системы. |
| 4. | Реализация системы защиты информации в информационной системе. | Реализация системы защиты информации в информационной системе. Установка и настройка средств защиты информации в информационной системе. Разработка документов, определяющих мероприятия, проводимые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации. Внедрение организационных мер в информационной системе. Предварительные испытания системы защиты информации информационной системы. Опытная эксплуатация системы защиты информации информационной системы. Анализ уязвимостей информационной системы. Приемочные испытания системы защиты информации информационной системы. |
| **8 семестр** | | |
| 1. | Аттестация информационной системы на соответствие требованиям о защите информации и ввод ее в действие. | Программа и методика аттестационных испытаний. Особенности аттестации информационной системы на основе результатов аттестационных испытаний выделенного набора ее сегментов. |
| 2. | Эксплуатация системы защиты | Обеспечение безопасности среды эксплуатации информационной системы. Администрирование системы защиты информации информационной системы. Реагирование на |

| | | |
|---|---|---|
| | информации информационной системы. | инциденты, связанные с нарушением требований о защите информации. Управление конфигурацией системы защиты информации информационной системы. Управление защитой информации в информационной системе. |
| 3. | Защита информации в ходе снятия с эксплуатации информационной системы. | Архивирование информации конфиденциального характера, содержащейся в информационной системе. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации. |

### 5.3. Лабораторный практикум

**Таблица 5**

| № п/п | Наименование раздела | Наименование лабораторных работ |
|---|---|---|
| **7 семестр** | | |
| 1. | Основы методологии проектирования информационных систем | **Лабораторная работа № 1.** Модели жизненного цикла. Методологии и технологии проектирования ИС. |
| 2. | Основы проектирования | **Лабораторная работа № 2.** Функциональная модель IDEF0 информационной системы. |
| 3. | Классификация информационной системы. | **Лабораторная работа № 3.** Определение актуальных угроз безопасности информации и разработка на их основе модели угроз. |
| 4. | AS -IS. TO -BE. | **Лабораторная работа № 4** Функциональная модель IDEF0 информационной системы. |
| 5. | Защита информации | **Лабораторная работа № 5** Состав мер по защите информации, обеспечивающих блокирование (нейтрализацию) актуальных угроз безопасности информации, и их содержание в соответствии с установленным классом защищенности информационной системы. Функциональная модель IDEF0 безопасной информационной системы. TO -BE. |
| **8 семестр** | | |
| 6. | Эксплуатационная документация на систему защиты информации информационной системы. | **Лабораторная работа № 6.** Эксплуатационная документация на систему защиты информации информационной системы. Тестирование системы защиты информации информационной системы. |

| | | |
|---|---|---|
| 7. | Установка и настройка средств защиты информации в информационной системе. | **Лабораторная работа № 6.** Разработка документов, определяющих мероприятия, проводимые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации. |
| 8. | Архивирование информации конфиденциального характера, содержащейся в информационной системе. | **Лабораторная работа № 8.** Уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации. |

**5.4. Практические (семинарские) занятия: нет**

**Таблица 6**

| № п/п | Наименование раздела дисциплины | Содержание раздела |
|---|---|---|
| **1.** | **-** | **-** |

**6. Самостоятельная работа студентов по дисциплине**

Способ организации самостоятельной работы: подготовка проекта по заданной тематике, в соответствии таблицы 7.

**Таблица 7**

| №№ п/п | Тематика докладов с презентациями |
|---|---|
| 1. | Общая структура классических технологий проектирования ППС |
| 2. | Основные фазы жизненного цикла программного обеспечения |
| 3. | Стратегическое планирование |
| 4. | Анализ основных областей деятельности организации |
| 5. | Анализ информационных потребностей |
| 6. | Определение требований к создаваемой системе |
| 7. | Выработка и оценка вариантов построения системы |
| 8. | Разработка эскизного (концептуального) проекта системы |
| 9. | Оценка эскизного проекта |
| 10. | Разработка пользовательской архитектуры |

| | |
|---|---|
| 11. | Проектирование сценариев диалога пользователя с системой |
| 12. | Структурное (логическое) проектирование ППС |
| 13. | Формирование полного перечня задач и определение связей между ними |
| 14. | Выбор методов и разработка алгоритмов решения задач. |
| 15. | Итеративная модель процесса разработки |
| 16. | Каскадная модель процесса разработки |
| 17. | Разработка функциональных спецификаций программ |
| 18. | Проектирование реализации (физическое проектирование) |
| 19. | Проектирование базы данных системы |
| 20. | Основные этапы (вехи) процесса разработки |

Преподаватель поясняет требования к оформлению работы, предлагает тематику самостоятельной работы с использованием программного обеспечения, согласованного с преподавателем. При защите самостоятельной работы студенту необходимо представить презентацию на выполненную работу с использованием ПО MS Power Point

### 6.2. Тематика курсовых проектов

Целью выполнения курсового проекта по дисциплине «Проектирование и эксплуатация защищенных информационных систем» является закрепление теоретических и практических знаний в области защиты информации. Тематика курсового проекта определяется приказом по вузу в соответствии с утвержденной темой ВКР.

При выполнении курсового проекта по дисциплине «Проектирование и эксплуатация защищенных информационных систем» перед студентом ставятся следующие задачи:

- систематизация и обобщение знаний, полученных при изучении дисциплины «Проектирование и эксплуатация защищенных информационных систем» и применение их в процессе решения конкретных задач в предметной области выпускной квалификационной работы;

- развитие навыков самостоятельной работы с научной литературой, справочными материалами, Интернет – ресурсам, уметь подбирать, систематизировать и анализировать материал;

- развитие умений на основе анализа результатов выполненной работы делать научно – обоснованные выводы и рекомендации;

- развитие навыков четко и понятно излагать мысли в регламентируемом объеме работы, правильно оформлять научную документацию, в том числе, курсовые проекты;

- расширение кругозора в области проектирования и управления защитой информации.

Написание и оформление курсового проекта выполняется по методическим указаниям кафедры.

**Учебно-методическое обеспечение для самостоятельной работы студентов:**

1. Петров А.А. Компьютерная безопасность. Криптографические методы защиты : монография / А. А. Петров. — 3-е изд. — Саратов : Профобразование, 2024. — 446 с. — ISBN 978-5-4488-0091-7. — Текст : электронный // Образовательная платформа IPR CMART : [сайт]. — URL: https://www.iprbookshop.ru/books/145915/details (дата обращения: 20.04.2026). — Режим доступа: для авторизир. пользователей.
2. Баланов А.Н. Защита информационных систем. Кибербезопасность : учебное пособие для вузов / А. Н. Баланов. — 2-е изд. — Санкт-Петербург : Лань, 2024. — 216 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/ (дата обращения: 20.04.2026). — Режим доступа: для авторизир. пользователей.
3. Сычев Ю.Н. Защита информации и информационная безопасность : учебное пособие для студентов высших учебных заведений, обучающихся по направлению подготовки 10.03.01 «Информационная безопасность» (квалификация (степень) «бакалавр») / Ю. Н. Сычев. — Москва : ИНФРА-М, 2023. — 199 с. — (Высшее образование). — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/ (дата обращения: 20.04.2026). — Режим доступа: для авторизир. пользователей.

## 7. Оценочные средства

### 7.1. Вопросы к рубежным аттестациям

***Седьмой семестр***

***Вопросы к первой рубежной аттестации:***

1. Основы методологии проектирования информационных систем.
2. Модели жизненного цикла. Методологии и технологии проектирования ИС.
3. Определение актуальных угроз безопасности информации и разработка на их основе модели угроз.
4. Классификация информационной системы.
5. Цель и задачи обеспечения защиты информации в информационной системе.
6. Перечень нормативных правовых актов, методических документов и национальных стандартов, требованиям которых должна соответствовать информационная система.
7. Перечень типов объектов защиты информационной системы.
8. Требования к мерам и средствам защиты информации, применяемым в информационной системе.

9. Определение субъектов доступа (пользователи, процессы и иные субъекты доступа) и объектов доступа (устройства, объекты файловой системы, запускаемые и исполняемые модули, объекты системы управления базами данных, объекты, создаваемые прикладным программным обеспечением, иные объекты доступа).
10. Состав мер по защите информации, обеспечивающих блокирование (нейтрализацию) актуальных угроз безопасности информации, и их содержание в соответствии с установленным классом защищенности информационной системы.
11. Организационные меры, виды и типы средств защиты информации. компиляторов, загрузчиков, сборщиков.
12. Написание исходного кода компиляторов, загрузчиков, сборщиков Отладка компиляторов, загрузчиков, сборщиков Реинжиниринг разработанных компиляторов, загрузчиков, сборщиков, драйвера устройства.
13. Логическая структура, состав (количество) и места размещения элементов системы защиты информации информационной системы.
14. Выбор сертифицированных средств защиты информации с учетом их совместимости с информационными технологиями и техническими средствами обработки информации, функций безопасности этих средств и особенностей их реализации, а также класса защищенности информационной системы.
15. Параметры настройки средств защиты информации, обеспечивающие реализацию мер по защите информации и блокирование (нейтрализацию) актуальных угроз безопасности информации, в том числе путем устранения возможных уязвимостей информационной системы.
16. Эксплуатационная документация на систему защиты информации информационной системы.
17. Тестирование системы защиты информации информационной системы.

***Вопросы ко второй рубежной аттестации:***

1. Реализация системы защиты информации в информационной системе
2. Установка и настройка средств защиты информации в информационной системе.
3. Разработка документов, определяющих мероприятия, проводимые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации.
4. Внедрение организационных мер в информационной системе.
5. Предварительные испытания системы защиты информации информационной системы.
6. Опытная эксплуатация системы защиты информации информационной системы.
7. Анализ уязвимостей информационной системы.
8. Приемочные испытания системы защиты информации информационной системы.

***7 семестр***

***Образцы билетов рубежных аттестаций:***

**Грозненский Государственный Нефтяной Технический Университет**
**им. акад. М.Д. Миллионщикова**
**Кафедра «Информатика и вычислительная техника»**
**Дисциплина «**Проектирование и эксплуатация защищенных информационных систем**»**
**1-я рубежная аттестация**
**Группа: Семестр: 7**
**Билет №**

1. Классификация информационной системы
2. Цель и задачи обеспечения защиты информации в информационной системе

**Преподаватель**_____

**Грозненский Государственный Нефтяной Технический Университет**
**им. акад. М.Д. Миллионщикова**
**Кафедра «Информатика и вычислительная техника»**
**Дисциплина «**Проектирование и эксплуатация защищенных информационных систем**»**
**2-я рубежная аттестация**
**Группа: Семестр: 7**
**Билет №**

1. Реализация системы защиты информации в информационной системе
2. Установка и настройка средств защиты информации в информационной системе

**Преподаватель**_____

***Восьмой семестр***

***Вопросы к первой рубежной аттестации:***

1. Программа и методика аттестационных испытаний.
2. Особенности аттестации информационной системы на основе результатов аттестационных испытаний выделенного набора ее сегментов.
3. Обеспечение безопасности среды эксплуатации информационной системы.
4. Администрирование системы защиты информации информационной системы.
5. Реагирование на инциденты, связанные с нарушением требований о защите информации.

***Вопросы ко второй рубежной аттестации:***

1. Управление конфигурацией системы защиты информации информационной системы.
2. Управление защитой информации в информационной системе.
3. Архивирование информации конфиденциального характера, содержащейся в информационной системе.
4. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

***Восьмой семестр***

***Образцы билетов рубежных аттестаций:***

**Грозненский Государственный Нефтяной Технический Университет**
**им. акад. М.Д. Миллионщикова**
**Кафедра «Информатика и вычислительная техника»**
**Дисциплина «**Проектирование и эксплуатация защищенных информационных систем**»**
**1-я рубежная аттестация**
**Группа: Семестр: 8**
**Билет №**

1. Администрирование системы защиты информации информационной системы
2. Реагирование на инциденты, связанные с нарушением требований о защите информаци

**Преподаватель**_____

**Грозненский Государственный Нефтяной Технический Университет**
**им. акад. М.Д. Миллионщикова**
**Кафедра «Информатика и вычислительная техника»**
**Дисциплина «**Проектирование и эксплуатация защищенных информационных систем**»**
**2-я рубежная аттестация**
**Группа: Семестр: 8**
**Билет №**

1. Управление защитой информации в информационной системе
2. Архивирование информации конфиденциального характера, содержащейся в информационной системе

**Преподаватель**_____

**7.2. Вопросы к зачету/экзамену**

***Вопросы к зачету:***

1. Основы методологии проектирования информационных систем.
2. Модели жизненного цикла. Методологии и технологии проектирования ИС.
3. Определение актуальных угроз безопасности информации и разработка на их основе модели угроз.
4. Классификация информационной системы.
5. Цель и задачи обеспечения защиты информации в информационной системе.
6. Перечень нормативных правовых актов, методических документов и национальных стандартов, требованиям которых должна соответствовать информационная система.
7. Перечень типов объектов защиты информационной системы.
8. Требования к мерам и средствам защиты информации, применяемым в информационной системе.
9. Определение субъектов доступа (пользователи, процессы и иные субъекты доступа) и объектов доступа (устройства, объекты файловой системы,

запускаемые и исполняемые модули, объекты системы управления базами данных, объекты, создаваемые прикладным программным обеспечением, иные объекты доступа).

10. Состав мер по защите информации, обеспечивающих блокирование (нейтрализацию) актуальных угроз безопасности информации, и их содержание в соответствии с установленным классом защищенности информационной системы.
11. Организационные меры, виды и типы средств защиты информации. компиляторов, загрузчиков, сборщиков.
12. Написание исходного кода компиляторов, загрузчиков, сборщиков Отладка компиляторов, загрузчиков, сборщиков Реинжиниринг разработанных компиляторов, загрузчиков, сборщиков, драйвера устройства.
13. Логическая структура, состав (количество) и места размещения элементов системы защиты информации информационной системы.
14. Выбор сертифицированных средств защиты информации с учетом их совместимости с информационными технологиями и техническими средствами обработки информации, функций безопасности этих средств и особенностей их реализации, а также класса защищенности информационной системы.
15. Параметры настройки средств защиты информации, обеспечивающие реализацию мер по защите информации и блокирование (нейтрализацию) актуальных угроз безопасности информации, в том числе путем устранения возможных уязвимостей информационной системы.
16. Эксплуатационная документация на систему защиты информации информационной системы.
17. Тестирование системы защиты информации информационной системы.
18. Реализация системы защиты информации в информационной системе
19. Установка и настройка средств защиты информации в информационной системе.
20. Разработка документов, определяющих мероприятия, проводимые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации.
21. Внедрение организационных мер в информационной системе.
22. Предварительные испытания системы защиты информации информационной системы.
23. Опытная эксплуатация системы защиты информации информационной системы.
24. Анализ уязвимостей информационной системы.
25. Приемочные испытания системы защиты информации информационной системы.

***Образец билета к зачету:***

**Грозненский Государственный Нефтяной Технический Университет**
**им. акад. М.Д. Миллионщикова**
**Кафедра «Информатика и вычислительная техника»**
**Дисциплина «**Проектирование и эксплуатация защищенных информационных систем**»**
**Группа: Семестр: 7**
**Билет №**

1. Организационные меры, виды и типы средств защиты информации. компиляторов, загрузчиков, сборщиков

2. Написание исходного кода компиляторов, загрузчиков, сборщиков Отладка компиляторов, загрузчиков, сборщиков Реинжиниринг разработанных компиляторов, загрузчиков, сборщиков, драйвера устройства

3. Логическая структура, состав (количество) и места размещения элементов системы защиты информации информационной системы

**Подпись преподавателя_____ Подпись заведующего кафедрой _____**

***Вопросы к экзамену (8 семестр)***

1. 1. Программа и методика аттестационных испытаний.
2. Особенности аттестации информационной системы на основе результатов аттестационных испытаний выделенного набора ее сегментов.
3. Обеспечение безопасности среды эксплуатации информационной системы.
4. Администрирование системы защиты информации информационной системы.
5. Реагирование на инциденты, связанные с нарушением требований о защите информации.
6. Управление конфигурацией системы защиты информации информационной системы.
7. Управление защитой информации в информационной системе.
8. Архивирование информации конфиденциального характера, содержащейся в информационной системе.
9. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

***Образец билета к экзамену:***

**Грозненский Государственный Нефтяной Технический Университет**
**им. акад. М.Д. Миллионщикова**
**Кафедра «Информатика и вычислительная техника»**
**Дисциплина «**Проектирование и эксплуатация защищенных информационных систем**»**
**Группа: Семестр: 7**
**Билет №**

1. Реагирование на инциденты, связанные с нарушением требований о защите информации
2. Управление конфигурацией системы защиты информации информационной системы
3. Управление защитой информации в информационной системе

**Подпись преподавателя_____ Подпись заведующего кафедрой _____**

**7.3. Текущий контроль**

**Образец типового задания для лабораторных занятий**

**Лабораторная работа № 4**

**Задания к работе**

Цель: Отправить созданное письмо с проверкой корректности его атрибутов.

Начальное состояние Выполнен ВИ «Создать новое письмо» или ВИ «Создать ответ на письмо».

Акторы - Пользователь

Основной сценарий

1. Пользователь выполняет команду отправки письма.
2. Программа проверяет, правильно ли заполнено поле «Адрес».
3. Если нет, программа сообщает об ошибке и отменяет отправку. Конец.
4. Если да, то программа проверяет, заполнено ли поле «Тема».
5. Если нет, программа выдает предупреждение, но не отменяет отправку.
6. Программа помещает письмо в папку «Исходящие» и отсылает его.
7. После отправки программа перемещает письмо в папку «Отправленные».

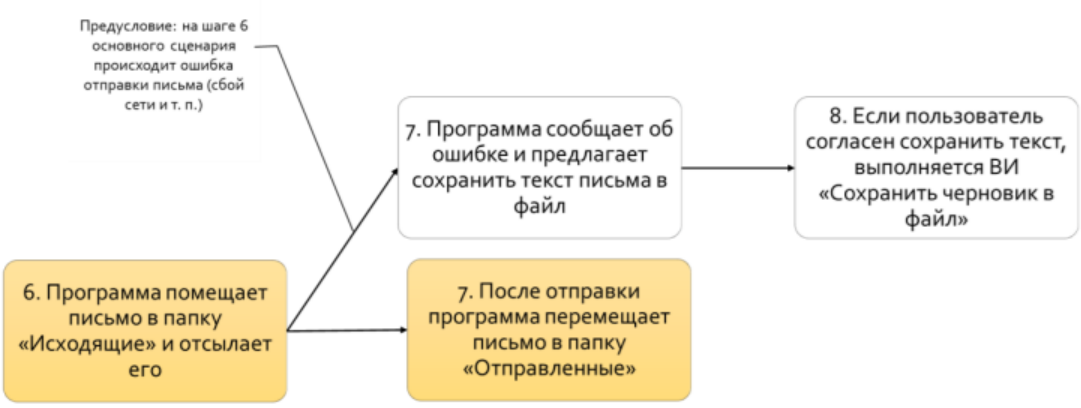


Рис. 1.2. Графическое изображение альтернативного сценария

Если альтернативных сценариев много и часть из них является терминальными (рис. 1.3), то описание всех альтернативных ВИ становится громоздким и сложным для восприятия.

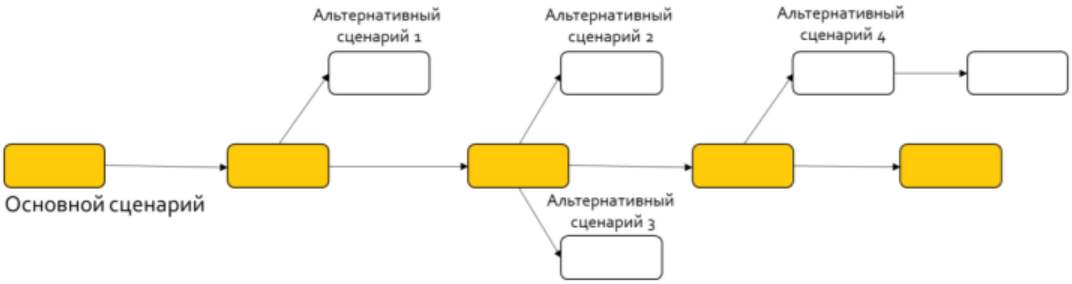


Рис. 1.3. Графическое изображение множества альтернативных сценариев

7.4. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкалы оценивания.

**7.4. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкалы оценивания**

**Таблица 8**

| **Планируемые результаты освоения компетенции** | **Критерии оценивания результатов обучения** | | | | **Наименование оценочного средства** |
|---|---|---|---|---|---|
| | **менее 41 баллов (неудовлетворительно)** | **41-60 баллов (удовлетворительно)** | **61-80 баллов (хорошо)** | **81-100 баллов (отлично)** | |
| **ОПК-6**<br>Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; | | | | | |
| **знать:**<br>- основные нормативные правовые акты, нормативные и методические документы Федеральной службы безопасности Российской Федерации,<br>Федеральной службы по техническому и экспортному контролю. | Фрагментарные знания | Неполные знания | Сформированные, но содержащие отдельные пробелы знания | Сформированные систематические знания | Билеты к рубежным аттестациям, билеты к зачету, билеты к экзамену, текущий |

| | | | | | |
|---|---|---|---|---|---|
| **уметь:**<br>- организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.<br>**владеть:**<br>- инструментарием, обеспечивающим программно-аппаратную защиту информационных ресурсов от изучения, модификации и копирования;<br>- навыками работы с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. | Частичное владение навыками | Несистематическое применение навыков | В систематическом применении навыков допускаются пробелы | Успешное и систематическое применение навыков | Частичное владение навыками |
| **ОПК-12**<br>Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений | | | | | |
| **знать:**<br>- основные исходные данные для проектирования подсистем. | Фрагментарные знания | Неполные знания | Сформированные, но содержащие отдельные пробелы знания | Сформированные систематические знания | Билеты к рубежным аттестациям, билеты к зачету, билеты к экзамену, текущий контроль |

| | | | | | |
|---|---|---|---|---|---|
| **уметь:**<br>- проводить экспериментальные исследования и проектировать подсистемы и средств обеспечения защиты информации.<br><br>**владеть:**<br>- методами технико-экономического обоснования соответствующих проектных решений. | Частичное владение навыками | Несистематическое применение навыков | В систематическом применении навыков допускаются пробелы | Успешное и систематическое применение навыков | Частичное владение навыками |
| **ПК-1.** Способен управлять защитой информации в автоматизированных системах | | | | | |
| **Знать:**<br>- основные угрозы безопасности информации и модели нарушителя<br>в автоматизированных системах; методы защиты информации от несанкционированного доступа и утечки по техническим каналам;<br>нормативные правовые акты в области защиты информации | Фрагментарные знания | Неполные знания | Сформированные, но содержащие отдельные пробелы знания | Сформированные систематические знания | Билеты к рубежным аттестациям, билеты к зачету, билеты к экзамену, текущий контроль |
| **Уметь:**<br>- определять подлежащие защите информационные ресурсы автоматизированных систем; оценивать информационные риски в автоматизированных системах; классифицировать и оценивать угрозы безопасности информации;<br>**Владеть:**<br>- методикой оценки последствий выявленных инцидентов и обнаружения нарушения правил разграничения доступа | Частичное владение навыками | Несистематическое применение навыков | В систематическом применении навыков допускаются пробелы | Успешное и систематическое применение навыков | Частичное владение навыками |
| ПК-2. Способен выполнять работы по установке, настройке и техническому обслуживанию защищенных технических средств обработки информации | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| **Знать:**<br>- основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; методы защиты информации от несанкционированного доступа и утечки по техническим каналам;<br>нормативные правовые акты в области защиты информации | Фрагментарные знания | Неполные знания | Сформированные, но содержащие отдельные пробелы знания | Сформированные систематические знания | Билеты к рубежным аттестациям, билеты к зачету, билеты к экзамену, текущий |
| **Уметь:**<br>- 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.<br>**Владеть:**<br>- методами защиты информации от несанкционированного доступа и специальных программных воздействий на нее. | Частичное владение навыками | Несистематическое применение навыков | В систематическом применении навыков допускаются пробелы | Успешное и систематическое применение навыков | Частичное владение навыками |

**8. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья**

Для осуществления процедур текущего контроля успеваемости и промежуточной аттестации обучающихся созданы фонды оценочных средств, адаптированные для инвалидов и лиц с ограниченными возможностями здоровья и позволяющие оценить достижение ими запланированных в основной образовательной программе результатов обучения и уровень сформированности всех компетенций, заявленных в образовательной программе. Форма проведения текущей аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.). При тестировании для слабовидящих студентов используются фонды оценочных средств с укрупненным шрифтом. На экзамен приглашается сопровождающий, который обеспечивает техническое сопровождение студенту. При необходимости студенту-инвалиду предоставляется дополнительное время для подготовки ответа на экзамене (или зачете). Обучающиеся с ограниченными возможностями здоровья и обучающиеся инвалиды обеспечиваются печатными и электронными образовательными ресурсами (программы, учебные пособия для самостоятельной работы и т.д.) в формах, адаптированных к ограничениям их здоровья и восприятия информации:

1) для инвалидов и лиц с ограниченными возможностями здоровья **по зрению:**

- **для слепых:** задания для выполнения на семинарах и практических занятиях оформляются рельефно-точечным шрифтом Брайля или в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением для слепых, либо зачитываются ассистентом; письменные задания выполняются на бумаге рельефно-точечным шрифтом Брайля или на компьютере со специализированным программным обеспечением для слепых либо надиктовываются ассистенту; обучающимся для выполнения задания при необходимости предоставляется комплект письменных принадлежностей и бумага для письма рельефно-точечным шрифтом Брайля, компьютер со специализированным программным обеспечением для слепых;

- **для слабовидящих:** обеспечивается индивидуальное равномерное освещение не менее 300 люкс; обучающимся для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; задания для выполнения заданий оформляются увеличенным шрифтом;

2) для инвалидов и лиц с ограниченными возможностями здоровья **по слуху:**

- **для глухих и слабослышащих:** обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающимся предоставляется звукоусиливающая аппаратура индивидуального пользования; предоставляются услуги сурдопереводчика;

- **для слепоглухих** допускается присутствие ассистента, оказывающего услуги тифлосурдопереводчика (помимо требований, выполняемых соответственно для слепых и глухих);

3) для лиц с тяжелыми нарушениями речи, глухих, слабослышащих лекции и семинары, проводимые в устной форме, проводятся в письменной форме;

4) для инвалидов и лиц с ограниченными возможностями здоровья, **имеющих нарушения опорно-двигательного аппарата:**

- для лиц с нарушениями опорно-двигательного аппарата, нарушениями

двигательных функций верхних конечностей или отсутствием верхних конечностей: письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту; выполнение заданий (тестов, контрольных работ), проводимые в письменной форме, проводятся в устной форме путем опроса, беседы с обучающимся.

## 9. Учебно-методическое и информационное обеспечение дисциплины

### Основная литература

1. Петров А.А. Компьютерная безопасность. Криптографические методы защиты : монография / А. А. Петров. — 3-е изд. — Саратов : Профобразование, 2024. — 446 с. — ISBN 978-5-4488-0091-7. — Текст : электронный // Образовательная платформа IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/145915/details (дата обращения: 20.04.2026). — Режим доступа: для авторизир. пользователей.

2. Баланов А.Н. Защита информационных систем. Кибербезопасность : учебное пособие для вузов / А. Н. Баланов. — 2-е изд. — Санкт-Петербург : Лань, 2024. — 216 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/ (дата обращения: 20.04.2026). — Режим доступа: для авторизир. пользователей.

3. Сычев Ю.Н. Защита информации и информационная безопасность : учебное пособие для студентов высших учебных заведений, обучающихся по направлению подготовки 10.03.01 «Информационная безопасность» (квалификация (степень) «бакалавр») / Ю. Н. Сычев. — Москва : ИНФРА-М, 2023. — 199 с. — (Высшее образование). — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/ (дата обращения: 20.04.2026). — Режим доступа: для авторизир. Пользователей

## 10. Материально-техническое обеспечение дисциплины

### 10.1. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Перечень материально-технических средств учебной аудитории для проведения занятий по дисциплине:

- учебная аудитория, доска;
- стационарные компьютеры;
- мультимедийный проектор;
- настенный экран.

### 10.2. Помещения для самостоятельной работы

Учебная аудитория для самостоятельной работы – 3-05.

Аудитория 3-05, интерактивная доска SB 480-H2-062616, проектор Smart v25, аппаратная Nettop.

**Методические указания по освоению дисциплины**
**«Проектирование и эксплуатация защищенных информационных систем»**

## 1. Методические указания для обучающихся по планированию и организации времени, необходимого для освоения дисциплины

Изучение рекомендуется начать с ознакомления с рабочей программой дисциплины, ее структурой и содержанием разделов (модулей), фондом оценочных средств, ознакомиться с учебно-методическим и информационным обеспечением дисциплины.

Дисциплина «Проектирование и эксплуатация защищенных информационных систем» состоит из нескольких связанных между собой разделов, обеспечивающих последовательное изучение материала.

Обучение по дисциплине «Проектирование и эксплуатация защищенных информационных систем» осуществляется в следующих формах:

1. Аудиторные занятия (лекции, лабораторные занятия).
2. Самостоятельная работа студента (подготовка к лекциям, лабораторным занятиям, работа над проектом, индивидуальная консультация с преподавателем).

Учебный материал структурирован и изучение дисциплины производится в тематической последовательности. Каждому лабораторному занятию и самостоятельному изучению материала предшествует лекция по данной теме. Обучающиеся самостоятельно проводят предварительную подготовку к занятию, принимают активное и творческое участие в обсуждении теоретических вопросов, разборе проблемных ситуаций и поисков путей их решения.

**Описание последовательности действий обучающегося:**

При изучении курса следует внимательно слушать и конспектировать материал, излагаемый на аудиторных занятиях. Для его понимания и качественного усвоения рекомендуется следующая последовательность действий:

1. После окончания учебных занятий для закрепления материала просмотреть и обдумать текст лекции, прослушанной сегодня, разобрать рассмотренные примеры (10–15 минут).
2. При подготовке к лекции следующего дня повторить текст предыдущей лекции, подумать о том, какая может быть следующая тема (10–15 минут).
3. В течение недели выбрать время для работы с литературой в электронной библиотечной системе (по 1 часу).
4. При подготовке к лабораторному занятию повторить основные понятия по теме, изучить примеры. Решая конкретную ситуацию, – предварительно понять, какой теоретический материал нужно использовать. Наметить план решения, попробовать на его основе решить 1–2 задачи.

## 2. Методические указания по работе обучающихся во время проведения лекций

Лекции дают обучающимся систематизированные знания по дисциплине, концентрируют их внимание на наиболее сложных и важных вопросах. Лекции обычно излагаются в традиционном или в проблемном стиле. Для студентов в большинстве случаев в проблемном стиле. Проблемный стиль позволяет стимулировать активную познавательную

деятельность обучающихся и их интерес к дисциплине, формировать творческое мышление, прибегать к противопоставлениям и сравнениям, делать обобщения, активизировать внимание обучающихся путем постановки проблемных вопросов, поощрять дискуссию.

Во время лекционных занятий рекомендуется вести конспектирование учебного материала, обращать внимание на формулировки и категории, раскрывающие суть того или иного явления, выводы и практические рекомендации.

Работая над конспектом лекций, необходимо использовать также литературу, которую дополнительно рекомендовал преподаватель. Тематика лекций дается в рабочей программе дисциплины.

**3. Методические указания обучающимся по подготовке к лабораторным занятиям**

На лабораторных занятиях приветствуется активное участие в обсуждении конкретных ситуаций, способность на основе полученных знаний находить наиболее эффективные решения задач, уметь находить полезный дополнительный материал по тематике занятий.

Студенту рекомендуется следующая схема подготовки к лабораторному занятию:

1. Ознакомиться с планом занятия, который отражает содержание предложенной темы.
2. Проработать конспект лекций.
3. Прочитать основную и дополнительную литературу.

В процессе подготовки к лабораторным занятиям, необходимо обратить особое внимание на самостоятельное изучение рекомендованной литературы. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов отношение к конкретной проблеме.

4. Выполнить домашнее задание.
5. При затруднениях сформулировать вопросы к преподавателю.

Результат такой работы должен проявиться в способности студента свободно ответить на теоретические вопросы, выступать и участвовать в коллективном обсуждении вопросов изучаемой темы, правильно выполнять практические задания, которые даются в фонде оценочных средств дисциплины.

**4. Методические указания обучающимся по организации самостоятельной работы**

Цель организации самостоятельной работы по дисциплине «Проектирование и эксплуатация защищенных информационных систем» – это углубление и расширение знаний в области проектирования и эксплуатации защищенных информационных систем; формирование навыка и интереса к самостоятельной познавательной деятельности.

Самостоятельная работа обучающихся является важнейшим видом освоения содержания дисциплины, подготовки к практическим занятиям и к рубежной аттестации. Самостоятельная работа носит исследовательский характер, что послужит в будущем

основанием для написания выпускной квалификационной работы, практического применения полученных знаний.

Организация самостоятельной работы обучающихся ориентируется на активные методы овладения знаниями, развитие творческих способностей, переход от поточного к индивидуализированному обучению, с учетом потребностей и возможностей личности.

Правильная организация самостоятельных учебных занятий, их систематичность, целесообразное планирование рабочего времени позволяет студентам развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивать высокий уровень успеваемости в период обучения, получить навыки повышения профессионального уровня.

Подготовка к лабораторному занятию включает, кроме проработки конспекта и презентации лекции, поиск литературы (по рекомендованным спискам и самостоятельно).

При подготовке к контрольной работе (рубежной аттестации) обучающийся должен повторять пройденный материал в строгом соответствии с учебной программой, используя конспект лекций и литературу, рекомендованную преподавателем. При необходимости можно обратиться за консультацией и методической помощью к преподавателю.

Самостоятельная работа реализуется:

– непосредственно в процессе аудиторных занятий – на лекциях, лабораторных занятиях;

– в контакте с преподавателем вне рамок расписания – на консультациях по учебным вопросам, в ходе творческих контактов, при ликвидации задолженностей, при выполнении индивидуальных заданий и т.д.

– в библиотеке, дома, на кафедре при выполнении обучающимся учебных и практических задач.

Виды СРС и критерии оценок

(по балльно-рейтинговой системе ГГНТУ, СРС оценивается в 15 баллов) 1. Проект с защитой

2. Подготовка к лабораторным занятиям

Темы для самостоятельной работы прописаны в рабочей программе дисциплины. Эффективным средством осуществления обучающимся самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к изданиям электронных библиотечных систем.

**Разработчик:**

Старший преподаватель кафедры
«Информатика и вычислительная техника» /Х.С. Халиева /

**СОГЛАСОВАНО:**

Зав.кафедрой «Информатика и
вычислительная техника» /_Э. Д. Алисултанова/

Директор ДУМР /Магомаева М.А./