МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

имени академика М.Д. Миллионщикова

«УТВЕРЖДАЮ»
Первый проректор-
проректор по ОД
_____ И.Т. Гайрабеков
«22» 06 2025г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«ЗАЩИТА ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ»

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 – 2025

Грозный – 2025

1. Цели и задачи дисциплины

Цель дисциплины состоит в изучении методов, механизмов и средств защиты информации в процессе ее обработки, хранения и передачи в компьютерных системах с учетом возможных угроз и требований нормативных документов.

Задача дисциплины:

- ознакомить студентов с основными проблемами защиты информации в компьютерных системах, а также с основными понятиями, используемыми при защите информации в компьютерных системах;

-обучить студентов методам защиты информации в компьютерных системах для построения защищенных информационных технологий.

2. Место дисциплины в структуре образовательной программы

Учебная дисциплина «Защита информационных процессов в компьютерных системах» относится к Блоку 1 части, формируемой участниками образовательных отношений учебного плана. Для изучения курса требуется освоение следующих дисциплин: «Основы информационной безопасности», «Основы управления информационной безопасностью.

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		
ПК-1. Способен управлять защитой информации в автоматизированных системах	**ПК-1.1. 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 **ПК-1.2. Уметь:** определять подлежащие защите информационные ресурсы автоматизированных систем; оценивать информационные риски в автоматизированных системах; классифицировать и оценивать угрозы безопасности информации; **ПК-1.3. Владеть:** методикой оценки последствий	**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 **Уметь:** определять подлежащие защите информационные ресурсы автоматизированных систем; оценивать информационные риски в автоматизированных системах; классифицировать и оценивать угрозы безопасности информации; **Владеть:** методикой оценки последствий выявленных инцидентов и обнаружения

	выявленных инцидентов и обнаружения нарушения правил разграничения доступа	нарушения правил разграничения доступа
ПК-4. Способен администрировать средства защиты информации прикладного и системного программного	**ПК-4.1. Знать:** порядок обеспечения безопасности информации при эксплуатации программного обеспечения; организационные меры по защите информации **ПК 4.2. Уметь**: формулировать правила безопасной эксплуатации программного обеспечения; обосновывать правила безопасной эксплуатации программного обеспечения; определять порядок функционирования программного обеспечения с целью обеспечения защиты информации; анализировать эффективность сформулированных требований к встроенным средствам защиты информации программного обеспечения **ПК 4.3. Владеть**: методикой формулирования требований к встроенным средствам защиты информации программного обеспечения	**Знать:** порядок обеспечения безопасности информации при эксплуатации программного обеспечения; организационные меры по защите информации **Уметь:** формулировать правила безопасной эксплуатации программного обеспечения; обосновывать правила безопасной эксплуатации программного обеспечения; определять порядок функционирования программного обеспечения с целью обеспечения защиты информации; анализировать эффективность сформулированных требований к встроенным средствам защиты информации программного обеспечения **Владеть:** методикой формулирования требований к встроенным средствам защиты информации программного обеспечения

4. Объем дисциплины и виды учебной работы

Таблица 2

Вид учебной работы	**Всего часов/ зач. ед.**		**Семестры**	
			7	**7**
	ОФО	**ОЗФО**	**ОФО**	**ОЗФО**
Контактная работа (всего)	**68/1,8**	**51/1,4**	**68/1,8**	**51/1,4**
В том числе:				
Лекции	34/0,9	17/0,5	34/0,9	17/0,5
Практические занятия	-	-	-	-
Семинары	-	-	-	-
Лабораторные работы	34/0,9	34/0,9	34/0,9	34/0,9
Самостоятельная работа (всего)	**84/2,2**	**101/2,8**	**84/2,2**	**101/2,8**
В том числе:				
Курсовая работа (проект)				
ИТР				

Рефераты		18/0,5	17/0,5	18/0,5	17/0,5
Работа над проектом		18/0,5	20/0,6	18/0,5	20/0,6
И (или) другие виды самостоятельной работы:					
Подготовка к лабораторным работам		18/0,5	30/0,8	18/0,5	30/0,8
Подготовка к практическим работам					
Подготовка к зачету					
Подготовка к экзамену		30/0,8	34/0,9	30/0,8	34/0,9
Контроль		**28/0,8**	**28/0,8**	**28/0,8**	**28/0,8**
Вид отчетности		**экзамен**	**экзамен**	**экзамен**	**экзамен**
Общая трудоемкость дисциплины	**ВСЕГО в часах**	**180**	**180**	**180**	**180**
	ВСЕГО в зач. единицах	**5**	**5**	**5**	**5**

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/з.е.	
		ОФО	ОЗФО	ОФО	ОЗФО	ОФО	ОЗФО
7 семестр							
1	Раздел 1. Введение	6	3	6	6	12	9
2	Раздел 2. Анализ возможных угроз в компьютерных системах	6	3	6	6	12	9
3	Раздел 3. Особенности защиты информационного процесса хранения данных	8	3	8	8	16	11
4	Раздел 4. Особенности защиты информационного процесса обработки данных	8	5	8	8	16	13
5	Раздел 5. Особенности защиты информационного процесса передачи данных	6	3	6	6	12	9

5.2. Лекционные занятия

Таблица 4

№ п/п	Наименование раздела дисциплины	Содержание раздела
1.	Раздел 1. Введение	Тема 1.1. Понятие информационного процесса. Классификация информационных процессов. Основные виды защищаемой информации. Тема 1.2. Понятие угрозы информационному процессу. Классификация угроз информационным процессам. Требования к защите

		данных в компьютерных системах
2.	Раздел 2. Анализ возможных угроз в компьютерных системах	Тема 2.1. Компьютерные системы и обеспечение их безопасности Архитектура сложных компьютерных систем с точки зрения обеспечения их безопасности Тема 2.2. Угрозы в компьютерных системах Основные угрозы информации в компьютерных системах. Специфика возникновения угроз в компьютерных сетях. Тема 2.3. Уязвимости в компьютерных системах Способы и средства анализа уязвимостей в компьютерных системах. Классификация компьютерных систем по возможным уязвимостям Тема 2.4. Каналы утечки информации в компьютерных системах Тема 2.5. Атаки на различных уровнях открытых систем. Возможности атаки на различных уровнях открытых систем. Аппаратные средства обеспечения безопасности открытых систем Тема 2.6. Алгоритмы проведения анализа и оценки угроз
3.	Раздел 3. Особенности защиты информационного процесса хранения данных	Тема 3.1. Характеристика и состав процесса хранения данных Системы хранения данных, архитектуры хранения данных, физические компоненты систем хранения данных. RAID-массивы. Интеллектуальные системы хранения данных. Сети хранения 7 данных Тема 3.2. Резервное копирование и восстановление Цель резервного копирования. Восстановление после отказа. Операционное резервное копирование. Архивирование. Тема 3.3. Репликация Локальная репликация. Технологии локальной репликации: на основе хоста, на основе массива хранения данных. Удаленная репликация. Режимы удаленной репликации. Технологии удаленной репликации: на основе хоста, на основе массива хранения данных, на основе SAN. Тема 3.4. Безопасность инфраструктуры хранения. Триада риска: активы, угрозы, уязвимости. Домены безопасности хранения. Безопасность области доступа к приложению: контроль доступа пользователя к данным, защита инфраструктуры хранения, шифрование данных. Безопасность области управления доступом: контроль административного доступа, защита инфраструктуры управления. Безопасность резервного копирования, восстановления и архивов. Тема 3.5. Внедрение безопасности в сети хранения. Архитектура безопасности SAN. Основные механизмы безопасности SAN. Тема 3.6. Мониторинг инфраструктуры хранения. Параметры для мониторинга. Мониторинг компонентов. Мониторинг доступности. Мониторинг безопасности.
4.	Раздел 4. Особенности защиты информационного	Тема 4.1. Характеристика и состав процесса обработки данных Схема процесса обработки данных, угрозы и уязвимости процесса Примеры процессов обработки

	процесса обработки данных	данных. Тема 4.2. Базовые технологии обеспечения безопасности процесса обработки данных. Кодирование данных. Программные закладки. Защита от изучения. Защита программ от несанкционированного копирования. Защита исполняемых файлов. Тема 4.3. Защита программ и данных в операционной системе Windows Тема 4.4. Защита программ и данных в операционных системах семейства Unix
5.	Раздел 5. Особенности защиты информационного процесса передачи данных	Тема 5.1. Характеристика и состав процесса передачи данных Архитектура процесса передачи данных. Угрозы и уязвимости процесса. Типичные проблемы безопасности в глобальных сетях на примере Интернет и локальных сетей предприятий. Тема 5.2. Базовые технологии обеспечения безопасности процесса передачи данных. Средства защиты информации в открытых сетях. Защита данных на канальном уровне. Защита данных на сетевом уровне. Тема 5.3.Основы построения виртуальных частных сетей Варианты технической реализации: на базе межсетевых экранов, маршрутизаторов, программного обеспечения, сетевой ОС, специализированных аппаратных средств. Тема 5.4. Межсетевые экраны Функции и назначение межсетевых экранов. Создание демилитаризованной зоны. Схемы подключения межсетевых экранов

5.3. Лабораторный практикум

Таблица 5

№ п/п	Наименование раздела	Наименование лабораторных работ
1.	Раздел 1. Введение	**Лабораторная работа №1.** Формирование модели угроз в информационной системе
2.	Раздел 2. Анализ возможных угроз в компьютерных системах	**Лабораторная работа №2.** Криптографическая защита данных на логических и физических дисках **Лабораторная работа №3.** Защита виртуальных дисков
3.	Раздел 3. Особенности защиты информационного процесса хранения данных	**Лабораторная работа №4.** Анализ и мониторинг возможных угроз в операционной системе Windows **Лабораторная работа №5.** Организация защищенного канала связи
4.	Раздел 4. Особенности защиты информационного процесса обработки данных	**Лабораторная работа №6.** Методы ограничения доступа к ресурсам АС **Лабораторная работа №7.** Настройка политики безопасности межсетевого экрана

5.	Раздел 5. Особенности защиты информационного процесса передачи данных	**Лабораторная работа №8.** Аттестация автоматизированных систем. Методика контроля **Лабораторная работа №9.** Реализация технологии виртуальных частных сетей

5.4. Практические занятия (семинары) – не предусмотрены.

Таблица 6

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

6. Самостоятельная работа

Способ организации самостоятельной работы: подготовка проекта по заданной тематике

Тематика докладов с презентациями

1. Защита от межсетевых атак
2. Анализ и предотвращение кибератак на компьютерные сети
3. Защита локальных сетей от внешних угроз
4. Использование биометрических технологий в системах безопасности
5. Разработка системы контроля доступа к информации в сетях
6. Анализ и прогнозирование угроз безопасности информации
7. Разработка методов обнаружения уязвимостей в операционных системах
8. Защита от хакерских атак на мобильные устройства
9. Создание системы резервного копирования и восстановления данных
10. Кибербезопасность государственных органов и крупных корпораций
11. Создание безопасной среды для онлайн-игр
12. Обнаружение и предотвращение внутренних угроз безопасности информации
13. Программное обеспечение для мониторинга безопасности сетей
14. Программное обеспечение для защиты от шпионского ПО
15. Методы обнаружения скрытых угроз в сети интернет Разработка средств защиты от вредоносных программ
16. Создание безопасной среды для обмена конфиденциальной информацией
17. Защита информации о компьютерных системах и сетях от утечек
18. Использование технологии ИИ для мониторинга безопасности сетей
19. Защита информации на промышленных объектах Обеспечение безопасности в использовании облачных сервисов
20. Разработка средств защиты от ARP-атак и DNS-фальсификации

Учебно-методическое обеспечение для самостоятельной работы студентов:

1. Фомин Д.В. Информационная безопасность : учебник / Д. В. Фомин. — Москва : Ай Пи Ар Медиа, 2022. — 222 с. — ISBN 978-5-4497-1548-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. —

URL: https://www.iprbookshop.ru/122687.html (дата обращения: 20.04.2025). — Режим доступа: для авторизир. пользователей.

2. Прохорова О.В. Информационная безопасность и защита информации : учебник для СПО / О. В. Прохорова. — 3-е изд., стер. — Санкт-Петербург : Лань, 2022. — 124 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/ (дата обращения: 20.04.2025). — Режим доступа: для авторизир. пользователей.

3. Бондаренко И.С. Информационная безопасность : учебник / И. С. Бондаренко. — Москва : Издательский Дом МИСиС, 2023. — 254 с. — ISBN 978-5-907560-71-0. — Текст : электронный // Образовательная платформа IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/137525/details (дата обращения: 20.04.2025). — Режим доступа: для авторизир. пользователей.

7. Оценочные средства

7.1. Вопросы к рубежным аттестациям

Седьмой семестр

Вопросы к первой рубежной аттестации:

1. Характеристика и состав процесса хранения данных
2. Архитектуры хранения данных.
3. Физические компоненты систем хранения данных.
4. Интеллектуальные системы хранения данных.
5. Сети хранения данных
6. Цель резервного копирования.
7. Восстановление после отказа.
8. Операционное резервное копирование.
9. Архивирование.
10. Локальная репликация.
11. Технологии локальной репликации.
12. Удаленная репликация. Режимы удаленной репликации.
13. Технологии удаленной репликации: на основе хоста, на основе массива хранения данных, на основе SAN.
14. Триада риска: активы, угрозы, уязвимости.
15. Домены безопасности хранения.
16. Архитектура безопасности SAN.
17. Основные механизмы безопасности SAN

Вопросы ко второй рубежной аттестации:

1. Параметры для мониторинга инфраструктуры хранения
2. Методы разграничения доступа к данным.
3. Особенности резервного копирования. Журналирование изменений.
4. Механизмы повышения защищённости, реализуемые в процессоре.
5. Механизмы повышения защищённости, реализуемые во внешних устройствах.
6. Механизмы защиты файловых систем.
7. Схема процесса обработки данных, угрозы и уязвимости процесса.
8. Базовые технологии обеспечения безопасности процесса обработки данных.

9. Архитектура процесса передачи данных. Угрозы и уязвимости процесса.
10. Типичные проблемы безопасности в глобальных сетях
11. Типичные проблемы безопасности локальных сетей предприятий.
12. Средства защиты информации в открытых сетях.
13. Защита данных на канальном уровне. ПК-2.3.4
14. Защита данных на сетевом уровне. ПК-2.3.4
15. Техническая реализация VPN на базе межсетевых экранов
16. Техническая реализация VPN на базе маршрутизаторов
17. Техническая реализация VPN на базе программного обеспечения

Образцы билетов рубежных аттестаций:

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информатика и вычислительная техника»
Дисциплина «Защита информационных процессов в компьютерных системах»
1-я рубежная аттестация
Группа: Семестр: 7
Билет №

1. Триада риска: активы, угрозы, уязвимости
2. Архитектура безопасности SAN

Преподаватель_____

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информатика и вычислительная техника»
Дисциплина «Защита информационных процессов в компьютерных системах»
2-я рубежная аттестация
Группа: Семестр: 7
Билет №

1. Защита данных на сетевом уровне. ПК-2.3.4)
2. Техническая реализация VPN на базе программного обеспечения

Преподаватель_____

7.2. Вопросы к экзамену
ОФО 7 семестр, ОЗФО 7 семестр

1. Характеристика и состав процесса хранения данных
2. Архитектуры хранения данных.
3. Физические компоненты систем хранения данных.
4. Интеллектуальные системы хранения данных.
5. Сети хранения данных
6. Цель резервного копирования.
7. Восстановление после отказа.
8. Операционное резервное копирование.
9. Архивирование.
10. Локальная репликация.
11. Технологии локальной репликации.

12. Удаленная репликация. Режимы удаленной репликации.
13. Технологии удаленной репликации: на основе хоста, на основе
14. массива хранения данных, на основе SAN.
15. Триада риска: активы, угрозы, уязвимости.
16. Домены безопасности хранения.
17. Архитектура безопасности SAN.
18. Основные механизмы безопасности SAN
19. Параметры для мониторинга инфраструктуры хранения.
20. Методы разграничения доступа к данным.
21. Особенности резервного копирования. Журналирование изменений.
22. Механизмы повышения защищённости, реализуемые в процессоре.
23. Механизмы повышения защищённости, реализуемые во внешних устройствах.
24. Механизмы защиты файловых систем.
25. Схема процесса обработки данных, угрозы и уязвимости процесса.
26. Базовые технологии обеспечения безопасности процесса обработки данных.
27. Архитектура процесса передачи данных. Угрозы и уязвимости процесса.
28. Типичные проблемы безопасности в глобальных сетях
29. Типичные проблемы безопасности локальных сетей предприятий.
30. Средства защиты информации в открытых сетях.
31. Защита данных на канальном уровне. ПК-2.3.4
32. Защита данных на сетевом уровне. ПК-2.3.4
33. Техническая реализация VPN на базе межсетевых экранов
34. Техническая реализация VPN на базе маршрутизаторов
35. Техническая реализация VPN на базе программного обеспечения

Образец билета к экзамену:

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информатика и вычислительная техника»
Дисциплина «Защита информационных процессов в компьютерных системах»
Группа: Семестр: 7
Билет №

1. Защита данных на канальном уровне. ПК-2.3.4
2. Типичные проблемы безопасности в глобальных сетях
3. Техническая реализация VPN на базе маршрутизаторов

Подпись преподавателя_____ Подпись заведующего кафедрой _____

7.3. Текущий контроль

Образец типового задания для лабораторных занятий

Лабораторная работа №1. Формирование модели угроз в информационной системе

Цель. Построение модели угроз безопасности защищаемого объекта информатизации.

Задачи

1) Определение перечня угроз безопасности объекта.

2) Анализ каналов утечки информации.

3) Построение модели угроз с учетом каналов утечки.

4) Разработка модели вероятного нарушителя.

Определение перечня угроз безопасности объекта

Угроза - потенциальная возможность совершения действий направленных на нарушение безопасности объекта.

Проявление угроз (фактор неопределенности):

– действие нарушителей;

– воздействие стихийных сил;

– сбои в работе средств СФЗ;

– воздействие субъективного фактора.

Исходными данными для проведения оценки и анализа служат результаты анкетирования субъектов отношений, направленные на уяснение направленности их деятельности, предполагаемых приоритетов целей безопасности, задач, решаемых на объекте и условий расположения и эксплуатации объекта.

Для составления перечня угроз необходимо:

– определить перечень актуальных источников угроз;

– определить перечень актуальных уязвимостей;

– оценить взаимосвязь угроз, источников угроз и уязвимостей;

– определить перечень возможных атак на объект;

– описать возможные последствия реализации угроз.

Угрозы утечки информации по техническим каналам.

1) Угрозы утечки речевой (акустической) информации по техническим каналам.

2) Характеристика угроз перехвата видовой (графической) информации ограниченного доступа визуальнооптическими средствами.

3) Угрозы утечки информации ограниченного доступа по каналам побочных электромагнитных излучений и наводок (ПЭМИН).

Технический канал утечки информации- совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Утечка информации- неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к ней и ее получения разведками.

Утечка (защищаемой) информации по техническим каналам -неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Основные элементы описания угроз утечки информации по техническим каналам представлены на рисунке 3.1.

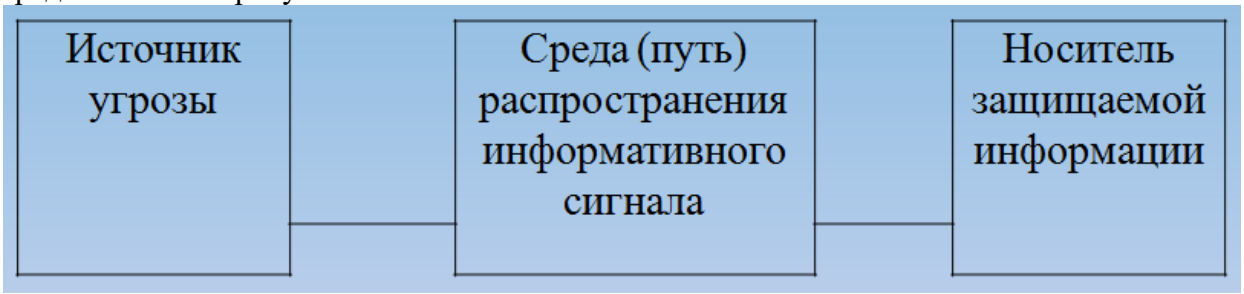

Рисунок 3.1 - Основные элементы угроз утечки информации

Носитель защищаемой информации - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде

символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Задание 1. Составить перечень угроз для заданного объекта по образцу таблицы 3.1.

Таблица 3.1 - Перечень угроз

№ угрозы	Источник угрозы	Среда распространения	Носитель информации

Каналы утечки информации по физическим принципам можно классифицировать на следующие группы:

- акустические (включая и акустопреобразовательные);
- визуально-оптические (наблюдение, фотографирование);
- электромагнитные (в том числе магнитные и электрические);
- материально-вещественные (бумага, фото, магнитные носители и т.п.).

При использовании технических средств для обработки и передачи информации возможны следующие каналы утечки и источники угроз безопасности информации:

– акустическое излучение информативного речевого сигнала;

– электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам, выходящими за пределы КЗ;

– виброакустические сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации защищаемых помещений;

– несанкционированный доступ и несанкционированные действия по отношению к информации в автоматизированных системах, в том числе с использованием информационных сетей общего пользования;

– воздействие на технические или программные средства информационных систем в целях нарушения конфиденциальности, целостности и доступности информации, работоспособности технических средств, средств защиты информации посредством специально внедренных программных средств;

– побочные электромагнитные излучения информативного сигнала от технических средств, обрабатывающих конфиденциальную информацию, и линий передачи этой информации;

– наводки информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы КЗ;

– радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств, при наличии паразитной генерации в узлах технических средств;

– радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств перехвата речевой информации "закладок", модулированные информативным сигналом;

– радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации;

– прослушивание ведущихся телефонных и радиопереговоров;

– просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей информации, в том числе с помощью оптических средств;

– хищение технических средств с хранящейся в них информацией или отдельных носителей информации.

Задание 2. Провести анализ потенциальных каналов утечки на указанном объекте. Составить перечень каналов утечки информации на защищаемом объекте с указанием места расположения по образцу таблицы 3.2.

Таблица 3.2 - Перечень потенциальных каналов утечки информации

Каналы утечки информации с объекта защиты			Место расположения
1.	Оптический канал	Окно со стороны проспекта	каб. №1
		Окно со стороны проспекта	каб. №2
		Окно со стороны проспекта	каб. №3
2.	Радиоэлектронный канал	Стоянка автотранспорта на просп.	указать
		Система часофикации	указать
		Телефон	указать
		Розетки	указать
		ПЭВМ	указать
		Воздушная линия электропередачи	указать
		Система оповещения	указать
		Система пожарной сигнализации	указать
3.	Акустический канал	Теплопровод подземный	указать
		Водопровод подземный	указать
		Стены помещения	указать
		Батареи	указать
		Окна контролируемого помещения	указать
4.	Материально-вещественный канал	Документы на бумажных носителях	указать
		Персонал предприятия	указать
		Производственные отходы	указать

Моделирование угроз безопасности информации предусматривает анализ способов её хищения, изменения, уничтожения с целью оценки наносимого ущерба. Моделирование угроз включает моделирование:

– способов физического проникновения;

– технических каналов утечки информации.

Возможные пути проникновения злоумышленника отмечаются на планах, схемах территорий, этажей помещений линиями. Результаты оформить в виде следующей модели, показанной в таблице 3.3.

Таблица 3.3 – Модель угроз защищаемого объекта

№ элемента	Цена информации	Путь проникновения	Оценка реальности	Величина угрозы	Ранг угрозы

Под утечкой информации понимается несанкционированный процесс переноса информации от источника к злоумышленнику.

Моделирование технических каналов утечки информации (ТКУИ) является единственным методом достаточно полного исследования их возможностей с целью последующей разработки способов и средств защиты. Целесообразно рассматривать каналы в статике и динамике. Статическое состояние характеризует пространственное состояние структурной модели, описывает состав и связи элементов канала утечки. Пространственная модель содержит описание положения канала утечки в пространстве:

места расположения источника и приёмника сигналов. Ориентация вектора распространения носителя информации в канале утечки и его протяжённость структурную модель целесообразно представить в табличной форме. Пространственную – в виде графов на планах помещений.

Динамику канала утечки описывает **функциональная и информационная модель.** Функциональная модель характеризует режимы функционирования канала: это может быть интервал времени, в течении которого возможна утечка. Информационная модель содержит характеристики информации, утечка которой возможна по техническому каналу(количество и ценность).

Указанные модели объединяются и увязываются между собой в рамках комплексной модели канала утечки. В ней указываются интегрированные параметры утечки – источник информации, его вид, источник сигнала, среда распространения, протяжённость среды распространения, возможное место размещения приёмника сигнала, информативность канала, величина угрозы. Все выявленные потенциальные каналы утечки и их характеристики заносятся в таблицу 3.4.

Таблица 3.4 – Комплексная модель каналов утечки

№	Цена информации	Источник сигнала	Путь утечки	Вид канала	Оценка реальности	Величина угрозы/ранг

Оценка угроз информации в результате проникновения злоумышленника к источнику или в результате её утечки по ТКУИ проводится с учётом вероятности реализуемости рассматриваемого пути или канала, а также с учётом цены соответствующего элемента информации. Угроза безопасности информации выражается в величине ущерба при захвате её злоумышленником, где - цена элемента информации - вероятность угрозы.

Задание 3. Построить модель угроз и комплексную модель каналов утечки информации для заданного объекта.

Под моделью нарушителя понимается совокупность количественных и качественных характеристик нарушителя, с учетом которых определяются требования к комплексу инженерно-технических средств охраны и/или его составным частям.

Составляющие модели нарушителя:

– категории нарушителя и его возможные тактические методы (внешние, внутренние, внешние в сговоре с внутренними);

– возможные действия нарушителя (применение силы, хищение, дезинформация и т.д.);

– причины и мотивы действий нарушителя (корысть, принуждение и т.д);

– возможности нарушителя (навык, опыт, количество, оснащенность-техника, оружие, транспорт).

«Внешний нарушитель» - нарушитель из числа лиц, не имеющих права доступа в охраняемые зоны;

«Внутренний нарушитель» - нарушитель из числа лиц, имеющих право доступа без сопровождения в охраняемые зоны;

«Внешняя угроза» - угроза, исходящая от внешнего нарушителя;

«Внутренняя угроза» - угроза, исходящая от внутреннего нарушителя.

Для описания моделей нарушителей в качестве критериев классификации рассматриваются:

1. Цели и задачи вероятного нарушителя:

- проникновение на охраняемый объект без причинения объекту видимого ущерба;

- причинение ущерба объекту;

- преднамеренное проникновение при отсутствии враждебных намерений;
- случайное проникновение.

2. Степень принадлежности вероятного нарушителя к объекту:
- вероятный нарушитель - сотрудник охраны;
- вероятный нарушитель - сотрудник учреждения;
- вероятный нарушитель - посетитель;
- вероятный нарушитель - постороннее лицо.

3. Степень осведомленности вероятного нарушителя об объекте:
- детальное знание объекта;
- осведомленность о назначении объекта, его внешних признаках и чертах;
- неосведомленный вероятный нарушитель.

4. Степень осведомленности нарушителя о системе охраны объекта:
- полная информация о системе охраны объекта;
- информация о системе охраны вообще и о системе охраны конкретного объекта охраны;
- информация о системе охраны вообще, но не о системе охраны конкретного объекта;
- неосведомленный вероятный нарушитель.

5. Степень профессиональной подготовленности вероятного нарушителя:
- специальная подготовка по преодолению систем охраны;
- вероятный нарушитель не имеет специальной подготовки по преодолению систем охраны.

6. Степень физической подготовленности вероятного нарушителя:
- специальная физическая подготовка;
- низкая физическая подготовка.

7. Владение вероятным нарушителем способами маскировки.

8. Степень технической оснащенности вероятного нарушителя.

9. Способ проникновения вероятного нарушителя на объект.

На основе изложенных критериев выделяют четыре категории нарушителя:

1) нарушитель первой категории - специально подготовленный по широкой программе, имеющий достаточный опыт нарушитель-профессионал с враждебными намерениями, обладающий специальными знаниями и средствами для преодоления различных систем защиты объектов;

2) нарушитель второй категории - непрофессиональный нарушитель с враждебными намерениями, действующий под руководством другого субъекта, имеющий определенную подготовку для проникновения на конкретный объект;

3) нарушитель третьей категории - нарушитель без враждебных намерений, совершающий нарушение безопасности объекта из любопытства или из каких-то иных личных намерений;

4) нарушитель четвертой категории - нарушитель без враждебных намерений, случайно нарушающий безопасность объекта.

Модели нарушителя по типу бывают: неформализованные, формализованные.

Неформализованная модель нарушителя представляет собой словесное описание его, отражает причины и мотивы действий, его возможности, априорные знания, преследуемые цели, их приоритетность для нарушителя, основные пути достижения поставленных целей, способы реализации исходящих от него угроз, место и характер действия, возможная тактика.

Формализованная модель нарушителя представляет собой математическое описание его, которое обычно строится на основе теории игр, когда для создания защитной системы используется матрица угроз/средств защит и матрица вероятностей наступления угроз. Типовая модель нарушителя представлена на рисунке 3.2.

Тип	Категория	Подготовленность								
		Психофизическая			Техническая			Осведомленность		
		Выс	Ср	Низк	Выс	Ср	Низк	Выс	Ср	Низк
Внешний	Специалист	+			+			+		
	Любитель		+			+			+	
	Дилетант			+			+			+
Внутренний	Сотрудник		+			+		+		

Рисунок 3.2 - Типовая модель нарушителя

Задание 4.

1) Провести анализ вероятных внешних и внутренних нарушителей.

2) Построить модель вероятного нарушителя (внешнего и внутреннего) на основе моделей угроз и утечки информации.

Варианты объектов защиты

№ варианта	Объект информатизации
1	Бухгалтерия завода железобетонных изделий
2	Помещения дирекции торгового центра
3	Медпункт учебного корпуса университета
4	Деканат факультета университета
5	Отдел главного конструктора приборного завода
6	Зал переговоров фирмы по изготовлению лекарственных средств
7	Следственный отдел прокуратуры
8	Помещение группы программистов коммерческого банка
9	Патентный отдел завода
10	Редакция научного издания
11	Отдел научно-исследовательского института
12	Помещения диссертационного совета университета
13	Рекламное агентство
14	Отдел кадров завода бурового оборудования
15	Конструкторское бюро завода оборонной промышленности

Контрольные вопросы

1 Что является исходными данными для проведения оценки и анализа угроз безопасности объектов?

2 Дать определение нарушителя, по каким критериям они классифицируются?

3 Дать определение технического канала утечки информации, назвать типы.

4 Дать определение носителя защищаемой информации, назвать типы.

5 Какие сведения включает пространственная модель каналов утечки?

6 Что такое формализованная и неформализованная модель нарушителя?

7 Перечислите цели и задачи вероятного нарушителя.

8 Какое оборудование относят к виброакустические каналам утечки информации?

9 Дать описание четырех категорий нарушителя.

10 Что представляет собой матрица угроз/средств защит и матрица вероятностей наступления угроз?

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

Таблица 7

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)**	
ПК-1. Способен управлять защитой информации в автоматизированных системах					
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	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	Билеты к зачету, текущий контроль
Уметь: определять подлежащие защите информационные ресурсы автоматизированных систем; оценивать информационные риски в автоматизированных системах; классифицировать и оценивать угрозы безопасности информации;	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть: методикой оценки последствий выявленных инцидентов и обнаружения нарушения правил разграничения доступа деятельности.	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются	Успешное и систематическое применение навыков	
ПК-4. Способен администрировать средства защиты информации прикладного и системного программного обеспечения					
Знать: порядок обеспечения безопасности информации при эксплуатации программного обеспечения; организационные меры по защите информации	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	Билеты к зачету, текущий контроль

Уметь: формулировать правила безопасной эксплуатации программного обеспечения; обосновывать правила безопасной эксплуатации программного обеспечения; определять порядок функционирования программного обеспечения с целью обеспечения защиты информации; анализировать эффективность сформулированных требований к встроенным средствам защиты информации программного обеспечения	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть: методикой формулирования требований к встроенным средствам защиты информации программного обеспечения деятельность по защите информации в сфере профессиональной деятельности.	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	

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. Фомин Д.В. Информационная безопасность : учебник / Д. В. Фомин. — Москва : Ай Пи Ар Медиа, 2022. — 222 с. — ISBN 978-5-4497-1548-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/122687.html (дата обращения: 20.04.2025). — Режим доступа: для авторизир. пользователей.

2. Прохорова О.В. Информационная безопасность и защита информации : учебник для СПО / О. В. Прохорова. — 3-е изд., стер. — Санкт-Петербург : Лань, 2022. — 124 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/ (дата обращения: 20.04.2025). — Режим доступа: для авторизир. пользователей.

3. Бондаренко И.С. Информационная безопасность : учебник / И. С. Бондаренко. — Москва : Издательский Дом МИСиС, 2023. — 254 с. — ISBN 978-5-907560-71-0. — Текст : электронный // Образовательная платформа IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/137525/details (дата обращения: 20.04.2025). — 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 – 3-07.

Аудитория 3-07, интерактивная доска SB 480-H2-062616, проектор Smart v25, аппаратная Nettop.

Методические указания по освоению дисциплины
«Защита информационных процессов в компьютерных системах»

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.

Обучение по дисциплине «Защита информационных процессов в компьютерных системах» осуществляется в следующих формах:

1. Аудиторные занятия (лекции, лабораторные занятия).
2. Самостоятельная работа студента (подготовка к лекциям, лабораторным занятиям, доклады с презентациями, 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.

Конспект лекции лучше подразделять на пункты, соблюдая красную строку. Этому в большой степени будут способствовать вопросы плана лекции, предложенные преподавателям. Следует обращать внимание на акценты, выводы, которые делает

преподаватель, отмечая наиболее важные моменты в лекционном материале замечаниями «важно», «хорошо запомнить» и т.п. Можно делать это и с помощью разноцветных маркеров или ручек, подчеркивая термины и определения.

Целесообразно разработать собственную систему сокращений, аббревиатур и символов. Однако при дальнейшей работе с конспектом символы лучше заменить обычными словами для быстрого зрительного восприятия текста.

Работая над конспектом лекций, необходимо использовать не только основную литературу, но и ту литературу, которую дополнительно рекомендовал преподаватель. Именно такая серьезная, кропотливая работа с лекционным материалом позволит глубоко овладеть теоретическим материалом.

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 поставленных проблем, 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. При всей полноте конспектирования лекции в ней невозможно изложить весь материал из-за лимита аудиторных часов. Поэтому 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. Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса.

1. Ответить на вопросы плана лабораторного занятия.
2. Выполнить домашнее задание.
3. 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 «Основы информационной безопасности» – это углубление и расширение знаний в области научной исследовательской деятельности; формирование навыка и интереса к самостоятельной познавательной деятельности.

Самостоятельная работа обучающихся является важнейшим видом освоения содержания дисциплины, подготовки к практическим занятиям и к контрольной работе. Сюда же относятся и самостоятельное углубленное изучение тем дисциплины.

Самостоятельная работа представляет собой постоянно действующую систему, основу образовательного процесса и 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), подготовку заготовок для выступлений по вопросам, выносимым для обсуждения по конкретной теме. Такие заготовки могут включать цитаты, факты, сопоставление различных позиций, собственные мысли. Если проблема заинтересовала обучающегося, он может подготовить реферат и выступить с ним на практическом занятии. Лабораторное занятие – это, прежде всего, дискуссия, обсуждение конкретной ситуации, то есть предполагает умение внимательно слушать членов малой группы и модератора, а также стараться высказать свое мнение, высказывать собственные идеи и предложения, уточнять и задавать вопросы коллегам по обсуждению.

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. Доклад с презентацией
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), лабораторных, к изданиям электронных библиотечных систем.

Разработчик:

Старший преподаватель кафедры
«Информатика и вычислительная техника»  /М.З. Исаева /

СОГЛАСОВАНО:

Зав. вып. каф.
«Информатика и вычислительная техника»  /Э. Д. Алисултанова/

Директор ДУМР  /М.А. Магомаева/