МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТИМЕНИ АКАДЕМИКА М.Д.МИЛЛИОНЩИКОВА»

Информационные технологии

УТВЕРЖДЕН

на заседании кафедры
«15» 05 2025 г., протокол № 9

Заведующий кафедрой
_____ Н.А. Моисеенко

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

«Безопасность информационных технологий и систем»

Направление подготовки
09.03.02 Информационные системы и технологии

Направленность (профиль)
«Информационные системы и технологии»
«Информационные технологии в образовании»
«Информационные технологии в дизайне»

Квалификация
бакалавр

Составитель (и) _____ И.Р. Усамов

Грозный – 2025

ПАСПОРТ

ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

«Безопасность информационных технологий и систем»

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемойкомпетенции (или ее части)	Наименование оценочного средства
1.	Основные понятия и анализ угроз информационной безопасности: политика безопасности	ОПК-3	Лабораторные работы Доклады с презентациями Письм. контрольная работа (аттестация) Экзамен
2.	Стандарты и спецификации в области информационной безопасности	ОПК-3	Лабораторные работы Доклады с презентациями Письм. контрольная работа (аттестация) Экзамен
3.	Угроза вредоносных программ и защита от них	ОПК-3	Лабораторные работы Доклады с презентациями Письм. контрольная работа (аттестация) Экзамен
4.	Безопасность вычислительных сетей	ОПК-3	Лабораторные работы Доклады с презентациями Письм. контрольная работа (аттестация) Экзамен

ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
1.	Лабораторная работа	Задания, выполняемые с использованием изучаемого программного обеспечения с целью углубления и закрепления теоретических знаний и развития навыков самостоятельного проведения эксперимента	Комплект заданий для выполнения лабораторных работ
2.	Доклад с презентацией	Продукт самостоятельной работы студента, представляющий собой публичное выступление по определенной учебно-практической, исследовательской или научной теме	Темы докладов
3.	Письм. контрольная работа (аттестация)	Подведение итогов учебной деятельности студентов в течение семестра в письменной форме	Вопросы по темам / разделам дисциплины
4.	Зачет	Итоговая форма оценки знаний	Вопросы к зачету

КОМПЛЕКТ ЗАДАНИЙ ДЛЯ ВЫПОЛНЕНИЯ ЛАБОРАТОРНЫХ РАБОТ

Лабораторные работы организуются в компьютерных аудиториях и выполняются по заданию преподавателя с использованием изучаемого программного обеспечения.

Тема 1. Разграничение прав пользователей

Определения понятий (изучить, включить в отчет):

- аутентификация,
- авторизация,
- администратор безопасности,
- симметричное и асимметричное шифрование,
- хеширование,
- политика безопасности.

Подготовить для включения в отчет о лабораторной работе ответы на следующие вопросы:

- какие существуют способы аутентификации пользователей?
- в чем слабость парольной аутентификации?
- как может быть повышена надежность аутентификации с помощью паролей?
- какой может быть реакция системы на попытку подбора паролей?
- кому может быть разрешен доступ по чтению и по записи к базе учетных записей пользователей?
- как должны храниться пароли в базе учетных записей пользователей?
- в чем смысл объединения пользователей в группы?

Тема 2. Реализация политики безопасности в защищенных версиях операционной системы Windows

Определение понятий (изучить, включить в отчет):

- аудит;
- событие безопасности;
- журнал (файл) аудита;
- политика аудита;
- интерактивный вход;
- сетевой доступ;
- домен компьютерной сети;
- цифровая подпись.

Подготовить для включения в отчет о лабораторной работе ответы на следующие вопросы:

- какие события безопасности должны фиксироваться в журнале аудита?
- какие параметры определяют политику аудита?
- целесообразно ли с точки зрения безопасности компьютерной системы объединение в одном лице функций администратора и аудитора?
- целесообразно ли с точки зрения безопасности компьютерной системы разрешать анонимный доступ к ее информационным ресурсам?
- как должен передаваться по сети (с точки зрения безопасности компьютерной системы) пароль пользователя (или другая аутентифицирующая информация)?
- нужно ли ограничивать права пользователей по запуску прикладных программ и почему?

Тема 3. Разграничение доступа к ресурсам в защищенных версиях операционной системы Windows

Подготовить для включения в отчет о лабораторной работе определения понятий:

- дискреционная политика безопасности;
- мандатная политика безопасности;
- субъект доступа;
- объект доступа;

- виды доступа;
- монитор обращений;
- монитор безопасности объектов;
- домен безопасности;
- реестр операционной системы;
- контроль целостности объектов;
- ключ симметричного шифрования;
- ключи асимметричного шифрования.

Подготовить для включения в отчет о лабораторной работе ответы на следующие вопросы:

- в чем достоинства и недостатки дискреционной политики безопасности?
- в чем достоинства и недостатки мандатной политики безопасности?
- в чем заключается тождественность объектов и тождественность субъектов компьютерной системы?
- кто определяет права доступа к папкам, файлам, принтерам при использовании дискреционной политики безопасности?
- каковы возможные пути нарушения политики безопасности в компьютерной системе?
- какие факторы влияют на определение размеров доменов безопасности?
- какая информация хранится в реестре Windows?

Тема 4. Использование программных средств контроля и анализа выполнения политики безопасности на примере операционной системы Windows XP/7

Подготовить для включения в отчет о лабораторной работе определения понятий:

- матрица доступа;
- дискреционный список контроля доступа;
- домен безопасности;
- журнал (файл) аудита;
- запись журнала аудита;
- стандарт безопасности.

Подготовить для включения в отчет о лабораторной работе ответы на следующие вопросы:

- что такое Trusted Computer System Evaluation Criteria (TCSEC)?
- какие основные категории требований к защищенности компьютерных систем предложены в TCSEC, в чем их смысл?
- какие требования к компьютерным системам предъявляются по классу защиты C2 TCSEC?
- кто управляет дискреционным списком контроля доступа к объектам в операционной системе Windows XP?
- как должны использоваться записи журнала аудита событий безопасности?
- какие права доступа к файлу аудита имеет по умолчанию администратор системы?
- что такое консольное приложение Windows?

Тема 5. Использование программных средств контроля и анализа выполнения политики безопасности на примере операционной системы Windows XP

Цель работы: освоение системных программ Windows XP, программ из комплекта Windows NT Resource Kit и других программных средств, предназначенных для:

- просмотра и управления разрешениями на доступ к конфиденциальным объектам компьютерной системы;
- просмотра и анализа записей аудита;
- анализа соответствия реализуемой в компьютерной системе политики безопасности требованиям стандартов безопасности;

- дополнительной защиты базы учетных записей пользователей компьютерной системы и используемых ими рабочих станций.

Подготовить для включения в отчет о лабораторной работе ответы на следующие вопросы:

- что такое Trusted Computer System Evaluation Criteria (TCSEC)?
- какие основные категории требований к защищенности компьютерных систем предложены в TCSEC, в чем их смысл?
- какие требования к компьютерным системам предъявляются по классу защиты C2 TCSEC?
- кто управляет дискреционным списком контроля доступа к объектам в операционной системе Windows XP?
- как должны использоваться записи журнала аудита событий безопасности?
- какие права доступа к файлу аудита имеет по умолчанию администратор системы?
- что такое консольное приложение Windows?

Наивысшая оценка лабораторной работы предусматривается в диапазоне от 2 до 5 баллов, в зависимости от сложности задания.

При оценке работы студента учитываются:

- уверенность действий при работе с изучаемым программным обеспечением;
- правильность выполнения необходимых шагов в лабораторной работе и адекватность / корректность полученного результата;
- умение самостоятельно находить способы решения возникающих проблем с помощью изучаемого программного обеспечения;
- способность ответить на вопросы преподавателя о последовательности выполненных шагов для получения результата.

ТЕМЫ ДОКЛАДОВ С ПРЕЗЕНТАЦИЯМИ

Подготовка презентации на 12-15 слайдов с устным докладом по заданной тематике:

Примерный перечень тем:

1. ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» Части 1, 2, 3
2. Анализ методов повышения надежности хранения информации на жестких магнитных дисках
3. Анализ средств защиты от спама
4. Анализ методов обеспечения безопасности домашней сети
5. Анализ методов изучения поведения нарушителей безопасности компьютерных систем
6. Анализ методов перехвата паролей пользователей компьютерных систем и методов противодействия им
7. Сравнительный анализ антивирусных пакетов
8. Анализ методов обеспечения безопасности электронного магазина
9. Анализ методов организации антивирусной защиты компьютерных систем
10. Сравнительный анализ систем обнаружения атак
11. Анализ средств безопасности в пакете Microsoft Office
12. ГОСТ Р ИСО/МЭК ТО 15446 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности»
13. Сравнительный анализ средств защиты электронной почты
14. ГОСТ Р ИСО/МЭК ТО 19791 «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем».

Критерии оценки доклада с презентацией:

13-15 баллов выставляется студенту, если:

- проведенное исследование и изложенный в докладе материал соответствует заданной теме;
- представленные в докладе сведения отвечают требованиям актуальности и новизны;
- продумана структура и стиль сопроводительной презентации;
- студент способен ответить на вопросы преподавателя по теме доклада.

6-12 баллов:

- представленный в докладе материал соответствует заданной теме, однако присутствуют недостатки в связности изложения и структуре сопроводительной презентации;
- не все выводы носят аргументированный и доказательный характер.

1-5 баллов:

- студент способен изложить материал доклада, однако наблюдаются отклонения от заданной темы;
- сопроводительная презентация подготовлена, но плохо соотносится с представленным докладом.

0 баллов:

- материал не соответствует заданной теме;
- отсутствует сопроводительная презентация к докладу;

- студент не освоил материал полностью и не способен ответить на вопросы преподавателя по теме доклада.

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТИМЕНИ АКАДЕМИКА М.Д.МИЛЛИОНЩИКОВА

Институт _прикладных информационных технологий___

Кафедра ___Информационные технологии_____

Вопросы к экзамену по дисциплине «Безопасность информационных технологий и систем»

Итоговая отчетность студентов по дисциплине принимается по билетам, с предоставлением времени на подготовку (20-30 мин.) и последующим устным ответом преподавателю. Состав билета на зачет – 2 вопроса.

Вопросы к зачету

К 1-ой рубежной аттестации:

1. Основные понятия защиты информации и информационной безопасности. (ОПК-3)
2. Базовые свойства информации применительно к ИБ. (ОПК-3)
3. Идентификация, аутентификация, авторизация. (ОПК-3)
4. Анализ угроз ИБ. (ОПК-3)
5. Признаки классификации угроз. (ОПК-3)
6. НСД к информации. Способы получения НСД. (ОПК-3)
7. Общие критерии безопасности. (ОПК-3)
8. Концепции общих критериев. (ОПК-3)
9. Политика безопасности организации. (ОПК-3)
10. Распределение ролей и обязанностей администраторов и пользователей сети. (ОПК-3)
11. Структура политики безопасности. (ОПК-3)
12. Уровни политики безопасности. (ОПК-3)
13. Процедуры безопасности. (ОПК-3)

Ко 2-ой рубежной аттестации:

1. Основные понятия криптографической защиты информации. (ОПК-3)
2. Симметричные криптосистемы шифрования. (ОПК-3)
3. Ассиметричные криптосистемы шифрования. (ОПК-3)
4. Электронная цифровая подпись и функция хэширования. (ОПК-3)
5. Аутентификация, авторизация и администрирование действий пользователей. (ОПК-3)
6. Аутентификация на основе паролей. (ОПК-3)
7. Угрозы безопасности ОС. (ОПК-3)
8. Понятие защищенной ОС. (ОПК-3)
9. Основные функции подсистемы защиты ОС. (ОПК-3)
10. Разграничение доступа к объектам ОС. (ОПК-3)
11. Аудит. (ОПК-3)
12. Технология межсетевых экранов. (ОПК-3)
13. Функции МЭ. (ОПК-3)

14. Дополнительные возможности МЭ. (ОПК-3)
15. Проблемы безопасности МЭ. (ОПК-3)

При оценке ответа студента на экзамене учитываются:

- правильность ответа на вопрос;
- логика изложения материала вопроса;
- правильность ответа на дополнительные вопросы;
- умение увязывать теоретические и практические аспекты вопроса;
- культура устной речи студента.

В пределах допускаемых на экзамене 20 баллов студенту выставляется:

Более 15 баллов – студент показывает всестороннее глубокое систематическое знание учебно-методического материала, усвоил основную литературу и знаком с дополнительной литературой; самостоятельно, в логической последовательности и исчерпывающе отвечает на все вопросы билета; умеет анализировать, классифицировать, обобщать и систематизировать изученный материал, устанавливать причинно-следственные связи; увязывает теоретические аспекты предмета с практическими задачами.

От 6 до 15 баллов – студент обнаруживает, в основном, полное знание учебно-программного материала, успешно выполняет предусмотренные в программе задания; излагает ответы на поставленные вопросы систематизированно и последовательно, но имеются пробелы знаний в некоторых разделах; демонстрирует умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер; способен к самостоятельному пополнению и обновлению знаний в ходе дальнейшей учебной работы и профессиональной деятельности.

До 5 баллов – студент показывает знания основного учебно-программного материала в объеме, необходимом для дальнейшей учебы, знаком с основной литературой, рекомендованной программой, однако проявляет затруднения в самостоятельных ответах, оперирует неточными формулировками; в процессе ответов допускаются ошибки по существу вопросов. Студент способен решать лишь наиболее легкие задачи, владеет только обязательным минимумом практических навыков.

0 баллов – студент показывает существенные пробелы в знаниях основного учебного программного материала, допускает принципиальные ошибки в выполнении предусмотренных программой заданий; не способен ответить на вопросы билета даже при дополнительных наводящих вопросах преподавателя.

КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ «БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СИСТЕМ»

Билеты к рубежной аттестации

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Безопасность информационных технологий и систем»
1-я рубежная аттестация
Группа: **Семестр: 6**

Билет № 1

1. Основные понятия защиты информации и информационной безопасности
2. Политика безопасности организации

Подпись преподавателя_____ **Подпись заведующего кафедрой**_____

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Безопасность информационных технологий и систем»
1-я рубежная аттестация
Группа: **Семестр: 6**

Билет № 2

1. Распределение ролей и обязанностей администраторов и пользователей сети
2. Структура политики безопасности

Подпись преподавателя_____ **Подпись заведующего кафедрой**_____

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Безопасность информационных технологий и систем»
1-я рубежная аттестация
Группа: **Семестр: 6**

Билет № 3

1. Общие критерии безопасности
2. Процедуры безопасности

Подпись преподавателя_____ **Подпись заведующего кафедрой**_____

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Безопасность информационных технологий и систем»
1-я рубежная аттестация
Группа: **Семестр: 6**

Билет № 4

1. Структура политики безопасности
2. Общие критерии безопасности

Подпись преподавателя_____ **Подпись заведующего кафедрой**_____

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Безопасность информационных технологий и систем»
1-я рубежная аттестация
Группа: **Семестр: 6**

Билет № 5

1. Уровни политики безопасности
2. Процедуры безопасности

Подпись преподавателя_____ **Подпись заведующего кафедрой**_____

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Безопасность информационных технологий и систем»
1-я рубежная аттестация
Группа: **Семестр: 6**

Билет № 6

1. Процедуры безопасности
2. Идентификация, аутентификация, авторизация

Подпись преподавателя_____ **Подпись заведующего кафедрой**_____

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Безопасность информационных технологий и систем»
1-я рубежная аттестация
Группа: **Семестр: 6**

Билет № 7

1. Процедуры безопасности
2. Политика безопасности организации

Подпись преподавателя_____ **Подпись заведующего кафедрой**_____

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Безопасность информационных технологий и систем»
2-я рубежная аттестация
Группа: **Семестр: 6**

Билет № 1

1. Аутентификация на основе паролей
2. Основные понятия криптографической защиты информации

Подпись преподавателя_____ **Подпись заведующего кафедрой**_____

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Безопасность информационных технологий и систем»
2-я рубежная аттестация
Группа: **Семестр: 6**

Билет № 2

1. Угрозы безопасности ОС
2. Симметричные криптосистемы шифрования

Подпись преподавателя_____ **Подпись заведующего кафедрой**_____

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Безопасность информационных технологий и систем»
2-я рубежная аттестация
Группа: **Семестр: 6**

Билет № 3

1. Аутентификация, авторизация и администрирование действий пользователей
2. Технология межсетевых экранов

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Безопасность информационных технологий и систем»
2-я рубежная аттестация
Группа: **Семестр: 6**

Билет № 4

1. Угрозы безопасности ОС
2. Аудит

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Безопасность информационных технологий и систем»
2-я рубежная аттестация
Группа: **Семестр: 6**

Билет № 5

1. Аутентификация, авторизация и администрирование действий пользователей
2. Угрозы безопасности ОС

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Безопасность информационных технологий и систем»
2-я рубежная аттестация
Группа: **Семестр: 6**

Билет № 6

1. Основные понятия криптографической защиты информации
2. Понятие защищенной ОС

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Безопасность информационных технологий и систем»
2-я рубежная аттестация
Группа: **Семестр: 6**

Билет № 7

1. Электронная цифровая подпись и функция хэширования
2. Аутентификация, авторизация и администрирование действий пользователей

Подпись преподавателя_____ **Подпись заведующего кафедрой**_____

ЗАЧЕТНО-ЭКЗАМЕНАЦИОННЫЕ МАТЕРИАЛЫ

6 СЕМЕСТР, ЗАЧЕТ

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Безопасность информационных технологий и систем»
Группа: **Семестр: 6**

Билет № 1

1. Технология межсетевых экранов
2. Основные понятия криптографической защиты информации

Подпись преподавателя_____ **Подпись заведующего кафедрой**_____

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Безопасность информационных технологий и систем»
Группа: **Семестр: 6**

Билет № 2

1. Угрозы безопасности ОС
2. Процедуры безопасности

Подпись преподавателя_____ **Подпись заведующего кафедрой**_____

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Безопасность информационных технологий и систем»
Группа: **Семестр: 6**

Билет № 3

1. Политика безопасности организации
2. Аутентификация на основе одноразовых паролей

Подпись преподавателя_____ **Подпись заведующего кафедрой**_____

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Безопасность информационных технологий и систем»
Группа: **Семестр: 6**

Билет № 4

1. Основные понятия защиты информации и информационной безопасности
2. Дополнительные возможности МЭ

Подпись преподавателя_____ **Подпись заведующего кафедрой**_____

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Безопасность информационных технологий и систем»
Группа: **Семестр: 6**

Билет № 5

1. Структура политики безопасности
2. НСД к информации. Способы получения НСД

Подпись преподавателя_____ **Подпись заведующего кафедрой**_____

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Безопасность информационных технологий и систем»
Группа: **Семестр: 6**

Билет № 6

1. 1. Основные понятия защиты информации и информационной безопасности
2. Распределение ролей и обязанностей администраторов и пользователей сети

Подпись преподавателя_____ **Подпись заведующего кафедрой**_____

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Безопасность информационных технологий и систем»
Группа: **Семестр: 6**

Билет № 7

1. Функции МЭ
2. Основные функции подсистемы защиты ОС

Подпись преподавателя_____ **Подпись заведующего кафедрой**_____

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Безопасность информационных технологий и систем»
Группа: **Семестр: 6**

Билет № 8

1. Дополнительные возможности МЭ
2. Распределение ролей и обязанностей администраторов и пользователей сети

Подпись преподавателя_____ **Подпись заведующего кафедрой**_____

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Безопасность информационных технологий и систем»
Группа: **Семестр: 6**

Билет № 9

1. Процедуры безопасности
2. Понятие защищенной ОС

Подпись преподавателя_____ **Подпись заведующего кафедрой**_____

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Безопасность информационных технологий и систем»
Группа: **Семестр: 6**

Билет № 10

1. 2. Базовые свойства информации применительно к ИБ
2. Электронная цифровая подпись и функция хэширования

Подпись преподавателя_____ **Подпись заведующего кафедрой**_____

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Безопасность информационных технологий и систем»
Группа: **Семестр: 6**

Билет № 11

1. Аутентификация на основе PIN-кода
2. 1. Основные понятия защиты информации и информационной безопасности

Подпись преподавателя_____ **Подпись заведующего кафедрой**_____

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Безопасность информационных технологий и систем»
Группа: **Семестр: 6**

Билет № 12

1. Уровни политики безопасности
2. Аутентификация, авторизация и администрирование действий пользователей

Подпись преподавателя_____ **Подпись заведующего кафедрой**_____

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Безопасность информационных технологий и систем»
Группа: **Семестр: 6**

Билет № 13

1. 4. Анализ угроз ИБ
2. Аутентификация на основе PIN-кода

Подпись преподавателя_____ **Подпись заведующего кафедрой**_____

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Безопасность информационных технологий и систем»
Группа: **Семестр: 6**

Билет № 14

1. Разграничение доступа к объектам ОС
2. Структура политики безопасности

Подпись преподавателя_____ **Подпись заведующего кафедрой**_____