

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Минцаев Марат Шамалович
Должность: Ректор
Дата подписания: 23.11.2020 12:00:02
Уникальный программный ключ:
236bcc35c296f119d6aafdc22836b21db52dbc07971a88865a382519a4304cc

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

«УТВЕРЖДАЮ»
Первый проректор
И.Г. Гаирабеков



« 01 » 09 2020 г.

РАБОЧАЯ ПРОГРАММА
дисциплины
«Информационная безопасность и защита информации»

Направление подготовки
09.03.01 Информатика и вычислительная техника
Профиль подготовки

Квалификация выпускника
Бакалавр

1. Цели и задачи дисциплины

Дисциплина «Информационная безопасность и защита информации» предназначена для изучения принципов информационной безопасности государства, подходов к анализу его информационной инфраструктуры, принципов организации, проектирования и анализа систем защиты информации, освоения основ их комплексного построения на различных уровнях защиты и особенностей степеней защиты для государственного и частного назначения.

Дисциплина закладывает набор базовых знаний, которые позволят выпускникам адаптироваться в условиях бурного развития информационных технологий. Обучение студентов данному курсу способствует воспитанию у них стремления к постоянному повышению профессиональной компетентности, расширению профессионального кругозора, умения ориентироваться в тенденциях и направлениях развития комплексной защиты информации.

Задачи дисциплины - дать знания:

- основ комплексного обеспечения защиты информации и информационной безопасности;
- основ организационно-правового обеспечения защиты информации и информационной безопасности.

2. Место дисциплины в структуре образовательной программы

Дисциплина относится к вариативной части профессионального цикла. Для изучения курса требуются знания информатики, операционных систем, информационных технологий, инфокоммуникационных систем и сетей.

Помимо самостоятельного значения, данная дисциплина является предшествующей для курсов: моделирование процессов и систем, управление данными, интеллектуальные системы и технологии.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-5).

- способностью разрабатывать модели компонентов информационных систем, включая модели баз данных и модели и интерфейсов «человек – электронно-вычислительная машина» (ПК-1);

проектно-технологическая деятельность:

В результате освоения дисциплины студент должен:

знать:

- содержание основных понятий обеспечения информационной безопасности;
- источники угроз безопасности информации, методы оценки уязвимости информации;
- методы пресечения разглашения конфиденциальной информации;
- виды и признаки компьютерных преступлений.

уметь:

- отыскивать необходимые нормативные правовые акты и информационные правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации;

- применять действующую законодательную базу в области обеспечения информационной безопасности и защиты информации;

- разрабатывать проекты положений, инструкций и других организационно-распорядительных документов, регламентирующих работу по защите информации.

владеть:

- навыками освоения и внедрения средств защиты информации;

- навыками сопровождения и управления системами защиты информации.

4. Объем дисциплины и виды учебной работы

Таблица 1

Вид учебной работы	Всего часов/ зач.ед.	
	ОФО	всего
	7 семестр	
Аудиторные занятия (всего)	68/2	68/2
В том числе:		
Лекции	34/1	34/1
Практические занятия		
Семинары		
Лабораторные работы	34/1	34/1
Самостоятельная работа (всего)	76/2	76/2
В том числе:		
Доклады	26/0,7	26/0,7
Презентации	26/0,7	26/0,7
<i>И (или) другие виды самостоятельной работы:</i>		
Подготовка к лабораторным работам	16/0,4	16/0,4
Подготовка к экзамену	8/0,2	8/0,2
Вид отчетности	экзамен	экзамен
Общая трудоемкость дисциплины	144	144
	4	4

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Таблица 2

№ п/п	Наименование раздела дисциплины по семестрам	Лекц. зан. часы	Лаб. зан. часы	Всего часов

1.	ОСНОВНЫЕ ПОНЯТИЯ И АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ПОЛИТИКА БЕЗОПАСНОСТИ	12	12	24
2.	СТАНДАРТЫ И СПЕЦИФИКАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	6	6	12
3.	УГРОЗА ВРЕДНОСНЫХ ПРОГРАММ И ЗАЩИТА ОТ НИХ	12	12	24
4.	БЕЗОПАСНОСТЬ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ	6	6	12

5.2. Лекционные занятия

Таблица 3

№ п/п	Наименование раздела дисциплины	Содержание раздела
1.	ОСНОВНЫЕ ПОНЯТИЯ И АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ПОЛИТИКА БЕЗОПАСНОСТИ	Понятие «Информационная безопасность». Составляющие информационной безопасности. Классификация угроз «информационной безопасности». Система формирования режима информационной безопасности. Административный уровень обеспечения информационной безопасности. Нормативно-правовые основы информационной безопасности в РФ.
2.	СТАНДАРТЫ И СПЕЦИФИКАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	Стандарты информационной безопасности: «Общие критерии». Стандарты информационной безопасности распределенных систем. Стандарты информационной безопасности в РФ.
3.	УГРОЗА ВРЕДНОСНЫХ ПРОГРАММ И ЗАЩИТА ОТ НИХ	Вирусы как угроза информационной безопасности. Классификация компьютерных вирусов. Характеристика «вирусоподобных» программ. Антивирусные программы. Профилактика компьютерных вирусов. Обнаружение неизвестного вируса.
4.	БЕЗОПАСНОСТЬ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ	Информационная безопасность вычислительных сетей. Механизмы обеспечения «информационной безопасности». Межсетевые экраны.

5.3. Лабораторный практикум

Таблица 4

№ п/п	Наименование раздела дисциплины	Наименование лабораторных работ
1.	ОСНОВНЫЕ ПОНЯТИЯ И АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ПОЛИТИКА БЕЗОПАСНОСТИ	Лабораторная работа №1. Разграничение прав пользователей
2.	ОСНОВНЫЕ ПОНЯТИЯ И АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ПОЛИТИКА БЕЗОПАСНОСТИ	Лабораторная работа №2. Реализация политики безопасности в защищенных версиях операционной системы Windows
3.	СТАНДАРТЫ И СПЕЦИФИКАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	Лабораторная работа №3. Разграничение доступа к ресурсам в защищенных версиях операционной системы Windows
4.	БЕЗОПАСНОСТЬ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ	Лабораторная работа №4. Использование программных средств контроля и анализа выполнения политики безопасности на примере операционной системы Windows XP/7
5.	УГРОЗА ВРЕДОНОСНЫХ ПРОГРАММ И ЗАЩИТА ОТ НИХ	Лабораторная работа №5. Использование программного продукта Acronis. Восстановление данных. Создание резервной копии пространства памяти
6.	УГРОЗА ВРЕДОНОСНЫХ ПРОГРАММ И ЗАЩИТА ОТ НИХ	Лабораторная работа №6. Использование программного продукта Acronis. Восстановление данных. Создание резервной копии пространства памяти

5.4. Практические занятия (семинары): планом не предусмотрены

Таблица 5

№ п/п	Наименование раздела дисциплины	Содержание раздела
1.		
2.		

6. Самостоятельная работа студентов по дисциплине

Подготовить доклад и презентацию по выбранной теме в области информационной безопасности (русский, зарубежный). Примерный перечень тем докладов:

- 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».

Перечень учебно-методического обеспечения для самостоятельной работы студентов:

1. Мельников, В.П. Информационная безопасность и защита информации: учеб. пособие для студ. высших учебных заведений [Текст] / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под ред. С.А. Клейменова – М.: Издательский центр «Академия», 2008. – 336 с. (www.library-it.ru)
2. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие [Текст] / В.Ф. Шаньгин. – М.: ИД «ФОРУМ»: ИНФРА-М, 2008. – 416 с.: ил. (библиотека ГГНТУ)

7. Фонды оценочных средств

Вопросы к 1 рубежной аттестации:

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

Вопросы ко 2 рубежной аттестации:

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

Вопросы к экзамену:

1. Основные понятия защиты информации и информационной безопасности
2. Базовые свойства информации применительно к ИБ
3. Идентификация, аутентификация, авторизация
4. Анализ угроз ИБ
5. Признаки классификации угроз
6. НСД к информации. Способы получения НСД
7. Общие критерии безопасности
8. Концепции общих критериев
9. Политика безопасности организации
10. Распределение ролей и обязанностей администраторов и пользователей сети
11. Структура политики безопасности
12. Уровни политики безопасности
13. Процедуры безопасности
14. Основные понятия криптографической защиты информации
15. Симметричные криптосистемы шифрования
16. Ассиметричные криптосистемы шифрования
17. Электронная цифровая подпись и функция хэширования
18. Аутентификация, авторизация и администрирование действий пользователей
19. Аутентификация на основе многофакторных паролей
20. Аутентификация на основе одноразовых паролей
21. Аутентификация на основе PIN-кода
22. Угрозы безопасности ОС
23. Понятие защищенной ОС
24. Основные функции подсистемы защиты ОС
25. Разграничение доступа к объектам ОС
26. Аудит
27. Технология межсетевых экранов
28. Функции МЭ

29. Дополнительные возможности МЭ

Образец билета к аттестации:

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Информационная безопасность и защита информации»
1 (2)-я рубежная аттестация
Группа: _____ Семестр: _____

Билет 1

1. Основные понятия защиты информации и информационной безопасности
2. Разграничение доступа к объектам ОС.

Преподаватель _____ Усамов И.Р.

Образец билета к экзамену:

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информационные технологии»
Дисциплина «Информационная безопасность и защита информации»
Группа: _____ Семестр: _____

Билет 1

1. Основные понятия защиты информации и информационной безопасности
2. Разграничение доступа к объектам ОС.

Преподаватель _____ Усамов И.Р.
Зав. кафедрой _____ Моисеенко Н.А.

Паспорт фонда оценочных средств дисциплины

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1.	ОСНОВНЫЕ ПОНЯТИЯ И АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ПОЛИТИКА БЕЗОПАСНОСТИ	ОПК-5 ПК-1	Письм. контрольная работа (аттестация) Обсуждение докладов

2.	СТАНДАРТЫ И СПЕЦИФИКАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	ОПК-5 ПК-1	Письм. контрольная работа (аттестация) Обсуждение докладов
3.	УГРОЗА ВРЕДОНОСНЫХ ПРОГРАММ И ЗАЩИТА ОТ НИХ	ОПК-5 ПК-1	Письм. контрольная работа (аттестация) Обсуждение докладов
4.	БЕЗОПАСНОСТЬ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ	ОПК-5 ПК-1	Письм. контрольная работа (аттестация) Обсуждение докладов

8. Учебно-методическое и информационное обеспечение дисциплины

Основная литература:

1. **Малюк, А.А.** Введение в информационную безопасность. Учебное пособие для вузов [Текст] / А.А. Малюк, В.И. Королев, В.М. Фомичев; Под ред. В.С. Горбатов. – М.: Горячая линия-Телеком, 2014. – 290 с.: ил. (библиотека ГГНТУ)

2. **Мельников, В.П.** Информационная безопасность и защита информации: учеб. пособие для студ. высших учебных заведений [Текст] / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под ред. С.А. Клейменова - М.: Издательский центр «Академия», 2008. – 336 с. (библиотека ГГНТУ)

3. **Шаньгин, В.Ф.** Информационная безопасность компьютерных систем и сетей. Учебное пособие [Текст] / В.Ф. Шаньгин. – М.: ИД «ФОРУМ»: ИНФРА-М, 2008. – 416 с.: ил. (библиотека ГГНТУ)

Дополнительная литература:

1. **Грибунин, В.Г.** Комплексная система защиты информации на предприятии. Учебное пособие [Текст] / В.Г. Грибунин, В.В. Чудовский - М.: Издательский центр «Академия», 2009. - 416 с. (библиотека ГГНТУ)

2. **Стрельцов, А.А.** Организационно-правовое обеспечение информационной безопасности. Учебное пособие для вузов [Текст] / А.А. Стрельцов, В.С. Горбатов, Т.А.Полякова, Т.А. Кондратьева, О. В. Дамаскин, Е. Б. Белов, С. Ю. Савин - М.: Академия, 2008. - 256 с. (библиотека ГГНТУ)

Интернет-ресурсы:

1. Информационно-образовательная среда кафедры «Информационные технологии» ГГНТУ [Электронный ресурс] // Режим доступа: <http://www.library-it.ru>

9. Материально-техническое обеспечение дисциплины

Компьютерный класс для проведения лабораторных занятий, интерактивная доска.

Разработчик:

Старший преподаватель кафедры
«Информационные технологии»



/ И.Р. Усамов /

Согласовано:

Зав. кафедрой
«Информационные технологии»



/ Н.А. Моисеенко /

Директор ДУМР



/ М.А. Магомаева /