МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

имени академика М.Д. Миллионщикова

«УТВЕРЖДАЮ»

Первый проректор

И.Г. Гайрабеков

«25» 01 2024г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Управление персоналом при обеспечении информационной безопасности»

Направление подготовки

10.03.01 Информационная безопасность

Направленность (профиль)

«Организация и технологии защиты информации»

Квалификация

бакалавр

Год начала подготовки – 2024

Грозный – 2024

1. Цели и задачи дисциплины

Целью изучения дисциплины «Управление персоналом при обеспечении информационной безопасности» является ознакомление студентов с терминологией управления информационной безопасностью; изучение студентами методов и средств обеспечения информационной безопасности; освоение навыками формирования требований к системе управления ИБ конкретного объекта, а также приобретение набора и профессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01 «Информационная безопасность».

Задача дисциплины - обеспечить освоение основ:

- Формирования требований к системе управления ИБ конкретного объекта.
- Проектирования системы управления ИБ конкретного объекта.
- Эффективного управления ИБ конкретного объекта.

2. Место дисциплины в структуре образовательной программы

Учебная дисциплина «Управление персоналом при обеспечении информационной безопасности» относится к Блоку 1 части, формируемой участниками образовательных отношений учебного плана. Для изучения курса требуется освоение следующих дисциплин: «Проектирование и эксплуатация защищенных информационных систем», «Методы и средства защиты информации в системах документооборота».

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)
профессиональные		
ПК-2. Способен выполнять работы по установке, настройке и техническому обслуживанию защищенных технических средств обработки информации;	ПК 2.1. Знать: технические описания и инструкции по эксплуатации технических средств обработки информации в защищенном исполнении, методы контроля защищенности информации от несанкционированного доступа и специальных программных воздействий, порядок аттестации объектов информатизации на соответствие требованиям безопасности ПК 2.2. Уметь: проводить настройку защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами, Проводить техническое обслуживание защищенных	Знать: роль информации в современном обществе, основы информационных технологий и информационной безопасности. Уметь: применять информационные технологии и основы информационной безопасности для обеспечения объективных потребностей личности, общества и государства. Владеть навыками использования информационных технологий и основ информационной безопасности для обеспечения объективных потребностей личности, общества и государства.

	технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-технической документацией. ПК 2.3. Владеть: методами защиты информации от несанкционированного доступа и специальных программных воздействий на нее	
ПК-3. Способен осуществлять аудит защищенности информации в автоматизированных системах	ПК-3.1. Знать: методы контроля эффективности защиты информации от несанкционированного доступа и утечки по техническим каналам; принципы построения систем защиты информации; организационные меры по защите информации ПК 3.2. Уметь: разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем; применять инструментальные средства контроля защищенности информации в автоматизированных системах ПК 3.3. Владеть: методами оценки информационных рисков безопасности информации в автоматизированной системе.	

4. Объем дисциплины и виды учебной работы

Таблица 2

Вид учебной работы	**Всего часов/ зач.ед.**	**ОФО**
	ОФО	8 сем.
Контактная работа	**48/1,3**	**48/1,3**

В том числе:		
Лекции	24/0,6	24/0,6
Лабораторные работы (ЛР)	24/0,8	24/0,8
Самостоятельная работа (всего)	**96/2,6**	**96/2,6**
В том числе:		
Расчетно-графические работы		
Темы для самостоятельного изучения	30/0,8	30/0,8
Подготовка презентаций	32/0,8	32/0,8
И(или) другие виды самостоятельной работы:		
Подготовка к лабораторным работам	-	-
Подготовка к зачету	34/0,9	34/0,9
Подготовка к экзамену		
Вид отчетности	зач	зач
Общая трудоемкость дисциплины Час. Зач. ед.	144 4	144 4

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Таблица 3

№ п/п	Наименование раздела дисциплины	Лекц.	Лаб.	Всего часов/з.е.
		ОФО	ОФО	ОФО
8 семестр				
1.	Предпосылки и основные направления развития менеджмента в сфере информационной безопасности	2	2	4/0,1
2.	Международные организации в сфере информационной безопасности	2	2	4/0,1
3.	Создание системы управления информационной безопасностью на предприятии	2	2	4/0,1
4.	Основы построения политики информационной безопасности на предприятии	2	2	4/0,1
5.	Безопасность информационных технологий предприятия	2	2	4/0,1
6.	Департамент информационной безопасности предприятия и работа с персоналом	2	2	4/0,1
7.	Аудит состояния информационной безопасности на предприятии	2	2	4/0,1
8.	Программные средства, поддерживающие управление информационной безопасностью на предприятии	2	2	4/0,1
9.	Организация реагирования на инциденты в сфере информационной безопасности	2	2	4/0,1
10.	Предоставление услуг в сфере информационной безопасности	2	2	4/0,1
11.	Управление информационной безопасностью на уровне крупных поставщиков информационных систем	2	2	4/0,1
12.	Управление информационной безопасностью на государственном уровне	2	2	4/0,1

5.2. Лекционные занятия

Таблица 4

№ п/п	Наименование раздела дисциплины	Содержание раздела
8 семестр		
1.	Предпосылки и основные направления развития менеджмента в сфере информационной безопасности	Предпосылки и основные направления развития менеджмента в сфере информационной безопасности 1. Предпосылки развития менеджмента в сфере информационной безопасности. 2. Основные направления развития менеджмента в сфере информационной безопасности
2.	Международные организации в сфере информационной безопасности	Международные организации в сфере информационной безопасности 1. Международные профессиональные объединения в сфере информационной безопасности. 2. Специализированные международные организации в сфере информационной безопасности
3.	Создание системы управления информационной безопасностью на предприятии	Создание системы управления информационной безопасностью на предприятии 1. Основные этапы разработки системы управления информационной безопасностью на предприятии. 2. Инвентаризация активов компании, категорирование активов компании. 3. Оценка защищенности информационной системы компании. Оценка и обработка информационных рисков. 4. Внедрение выбранных мер обработки рисков. Контроль выполнения и эффективности выбранных мер
4.	Основы построения политики информационной безопасности на предприятии	Основы построения политики информационной безопасности на предприятии 1. Основы обеспечения режима информационной безопасности на предприятии 1.50 - 2. Основы анализа информационных рисков компании 3. Формирование политики информационной безопасности на предприятии
5.	Безопасность информационных технологий предприятия	Безопасность информационных технологий предприятия 1. Способы управления безопасностью информационных технологий 2. Исходные данные и состав политики безопасности информационных технологий предприятия 3. Политика безопасности информационных технологий
6.	Департамент информационной безопасности предприятия и работа с персоналом	Департамент информационной безопасности предприятия и работа с персоналом 1. Назначение и функции департамента информационной безопасности предприятия 2. Организационная структура и персонал департамента информационной безопасности 3. Особенности работы с персоналом предприятия
7.	Аудит состояния информационной безопасности на предприятии	Аудит состояния информационной безопасности на предприятии 1. Назначение, цели и этапы аудита состояния информационной безопасности предприятия 2. Содержание основных этапов аудита состояния информационной безопасности предприятия 3. Анализ собранной информации и заключение при аудите состояния информационной безопасности предприятия
8.	Программные средства, поддерживающие управление информационной безопасностью на предприятии	Программные средства, поддерживающие управление информационной безопасностью на предприятии 1. Основы применения программных средств поддержки управления безопасностью 2. Программные средства поддержки работы с политикой безопасности предприятия 3. Программные средства поддержки анализа рисков 4. Программные средства поддержки управления безопасностью, интегрируемые в информационную систему предприятия
9.	Организация реагирования на инциденты в сфере информационной безопасности	Организация реагирования на инциденты в сфере информационной безопасности 1. Характеристика этапов реагирования на инциденты 2. Оценка ущерба от инцидента в сфере информационной безопасности
10.	Предоставление услуг в сфере информационной безопасности	Предоставление услуг в сфере информационной безопасности 1. Предпосылки развития рынка услуг по обеспечению информационной безопасности и его структура 2. Особенности некоторых видов услуг в сфере информационной безопасности 3. Страхование информационных рисков

11.	Управление информационной безопасностью на уровне крупных поставщиков информационных систем	Управление информационной безопасностью на уровне крупных поставщиков информационных систем 1. Общая методология организационного обеспечения информационной безопасности на уровне крупных поставщиков информационных систем 2. Организационное обеспечение информационной безопасности на уровне отдельных крупных компаний
12.	Управление информационной безопасностью на государственном уровне	Управление информационной безопасностью на государственном уровне 1. Предпосылки развития государственного управления в сфере информационной безопасности 2. Общая методология и структура организационного обеспечения информационной безопасности на уровне государств. 3. Общая политика России в сфере информационной безопасности. 4. Структура органов государственной власти, обеспечивающих информационную безопасность в РФ.

5.3. Лабораторный практикум

Таблица 5

№ п/п	Наименование раздела	Наименование лабораторных работ
8 семестр		
1.	Предпосылки и основные направления развития менеджмента в сфере информационной безопасности	**Лабораторная работа №1** Построение функциональной модели процессов обеспечения информационной безопасности с помощью графических нотаций.
2.	Международные организации в сфере информационной безопасности	**Лабораторная работа №2** Нормативно-правовые документы и стандарты в области защиты информации и информационной безопасности
3.	Создание системы управления информационной безопасностью на предприятии	**Лабораторная работа №3** Определение угроз безопасности информации в компьютерной системе организации
4.	Основы построения политики информационной безопасности на предприятии	**Лабораторная работа № 4** Анализ рынка и подбор средств для проекта СЗИ предприятия.
5.	Безопасность информационных технологий предприятия	**Лабораторная работа №5** Оценка рисков информационной безопасности компании на основе модели информационных потоков
6.	Департамент информационной безопасности предприятия и работа с персоналом	**Лабораторная работа №6** Изучение методов и средств обеспечения безопасности информационных и телекоммуникационных технологий
7.	Аудит состояния информационной безопасности на предприятии	**Лабораторная работа №7** Изучение методологии аудита информационной безопасности организации
8.	Программные средства, поддерживающие управление информационной безопасностью на предприятии	**Лабораторная работа №8** Контроль целостности программной среды.
9.	Организация реагирования на инциденты в сфере информационной безопасности	**Лабораторная работа №9** Определение потенциала нарушителя, необходимого для реализации угрозы безопасности информации
10.	Предоставление услуг в сфере информационной безопасности	**Лабораторная работа №10** Исследование предприятия по предоставлению услуг в сфере информационной безопасности
11.	Управление информационной безопасностью на уровне крупных поставщиков информационных систем	**Лабораторная работа №11** Изучение системы правление информационной безопасностью
12.	Управление информационной безопасностью на государственном уровне	**Лабораторная работа №12** Изучение государственных нормативных актов по управлению информационной безопасностью на государственном уровне

5.4. Практические занятия (семинары) – не предусмотрены.

6. Самостоятельная работа

6.1. Тематика и формы самостоятельной работы студентов

8 семестр

Таблица 6

№№ п/п	Тематика докладов с презентациями
1	Безопасность и правовое регулирование электронной коммерции
2	Обзор деятельности центров реагирования на инциденты в РФ
3	Обзор деятельности МСЭТ по управлению информационной безопасности
4	.Обзор материалов Гост Р ИСО/МЭК 18044 -2007 Менеджмент инцидентов информационной безопасности
5	Обзор материалов Гост ISO/IEC 27005-2012 Методы обеспечение безопасности. Менеджмент рисков безопасности
6	Менеджмент непрерывности бизнеса
7	Менеджмент оказание услуг третьим лицам и клиентам
8	Направления организационной работы в области безопасности, связанной с персоналом
9	Оценка эффективности передачи риска информационной безопасности третьим лицам
10	Мониторинг безопасности
11	Задачи департамента информационной безопасности
12	Аудит безопасности информационных технологий

Учебно-методическое обеспечение для самостоятельной работы студентов:

1. Шаньгин В.Ф. - Информационная безопасность и защита информации: учебное пособие - Саратов: Профобразование, 2017.

2. Мельников, В. П. Информационная безопасность и защита информации : [учеб. пособие] / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова. - 5-е изд., стер. - М. : Академия, 2011. - 336 с.: ил. - (Высшее профессиональное образование). - На учебнике гриф: Доп.УМО. - Библиогр.: с. 327-328. - ISBN 978-5-7695-7738-3

1. Оценочные средства

7.1. Вопросы к рубежным аттестациям

Первый семестр

Вопросы к 1ой рубежной аттестации:

1. Дайте понятие информационной безопасности в узком и широком смысле слова
2. Дайте определение рисков и охарактеризуйте их виды
3. Дайте определение угроз и охарактеризуйте их виды.
4. Охарактеризуйте основные наиболее распространенные способы нарушения информационной безопасности
5. Охарактеризуйте процесс обеспечения собственной информационной безопасности на предприятиях.
6. Укажите основные международные организации, действующие в сфере информационной безопасности и укажите решаемые ими задачи.
7. Опишите отличительные особенности крупных международных профессиональных (отраслевых) организаций (объединений).

8. Дайте определение системы управления информационной безопасностью (СУИБ) предприятия, приведите её состав и цели создания.
9. Основные этапы и условия разработки СУИБ.
10. Опишите организационную структуру менеджмента обеспечения информационной безопасности предприятия
11. Основные функции отдела информационной безопасности предприятия.
12. Сценарий анализа информационных рисков компании
13. Дайте определение и поясните смысл политики безопасности предприятия
14. Поясните основные этапы управления безопасностью информационных технологий.
15. Опишите процедуру оценки общего уровня риска при управлении безопасностью информационных технологий.
16. Дайте определение и раскройте задачи, решаемые департаментом информационной безопасности предприятия (ДИБП).
17. Опишите функции ДИБП, связанные с формированием, поддержкой и документальным обеспечением политики информационной безопасности предприятия.
18. Опишите функции ДИБП, с внедрением средств защиты информации.
19. Опишите функции ДИБП, связанные с администрированием информационных систем и систем защиты информации
20. Дайте определение аудита состояния информационной безопасности предприятия. Охарактеризуйте их виды.
21. Опишите цели и стратегическую задачу аудита состояния информационной безопасности предприятия.
22. Опишите требования к организациям, осуществляющим внешний аудит состояния информационной безопасности предприятия.
23. Основные этапы аудита состояния информационной безопасности предприятия и их характеристика
24. Охарактеризуйте процесс анализа действующей на предприятии политики безопасности.
25. Охарактеризуйте процесс изучения (проверки) действующих информационных ресурсов предприятия.

Образец билета к1-ой рубежной аттестации:

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Грозненский Государственный Нефтяной Технический Университет им. акад. М.Д. Миллионщикова
Кафедра «Информатика и вычислительная техника»
Дисциплина «Управление персоналом при обеспечении информационной безопасности»

1-я рубежная аттестация

Вариант 1

1. Дайте определение и поясните смысл политики безопасности предприятия
2. Опишите функции ДИБП, с внедрением средств защиты информации.

Преподаватель_____ _____ М.З.Исаева

Вопросы ко 2ой рубежной аттестации:

1. Виды программных средств поддержки реализации политики информационной безопасности.
2. Структура и краткое содержание отчета о состоянии информационной безопасности программного продукта «COBRA».
3. Дайте характеристику программного комплекса управления политикой информационной безопасности компании «КОНДОР+».
4. Предпосылки разработки политики безопасности предприятия.
5. Структура деятельности в сфере информационной безопасности. Основные задачи организационно-управленческой деятельности (менеджмента) в сфере информационной безопасности
6. Что включает в себя безопасная информационная инфраструктура?
7. Иерархия уровней организационной работы в сфере информационной безопасности и их характеристика
8. Охарактеризуйте этап разработки СУИБ: Оценка информационных рисков
9. Охарактеризуйте этап разработки СУИБ: Внедрение выбранных мер обработки рисков
10. Охарактеризуйте этап разработки СУИБ: Контроль выполнения и эффективности выбранных мер.
11. Охарактеризуйте верхний уровень политики информационной безопасности предприятия
12. Охарактеризуйте средний уровень политики информационной безопасности предприятия
13. Приведите перечень основных вопросов, входящих в состав политики безопасности информационных технологий.
14. Опишите функции ДИБП, связанные с контролем выполнения требований политики информационной безопасности и проведением аудитов.
15. Инструментальная проверка защищенности информационной системы предприятия.
16. Анализ собранной информации при аудите состояния информационной безопасности предприятия.
17. Содержание заключения при аудите состояния информационной безопасности предприятия.
18. Назначение программных средства, реализующих методологии анализа рисков.
19. Опишите назначение и возможности семейства программных продуктов "CRAMM".
20. Назначение и основные функции программных средств, интегрируемых в информационную систему предприятия.
21. Перечислите и охарактеризуйте известные программные средства, интегрируемые в информационную систему предприятия.
22. Дайте характеристику услуги первичной постановки системы управления информационной безопасностью.
23. Страхование в сфере информационной безопасности и основные объекты страхования.
24. Общая политика России в сфере информационной безопасности
25. Структура органов государственной власти, обеспечивающих информационную безопасность в РФ.

Образец билета к 2-ой рубежной аттестации:

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Грозненский Государственный Нефтяной Технический Университет им. акад. М.Д. Миллионщикова
Кафедра «Информатика и вычислительная техника»
Дисциплина «Управление персоналом при обеспечении информационной безопасности»

2-я рубежная аттестация

Вариант 1

1. Виды программных средств поддержки реализации политики информационной безопасности.
2. Общая политика России в сфере информационной безопасности

Преподаватель_____ _____ М.З. Исаева

7.2. Вопросы к зачету (3 семестр)

1. Дайте понятие информационной безопасности в узком и широком смысле слова
2. Дайте определение рисков и охарактеризуйте их виды
3. Дайте определение угроз и охарактеризуйте их виды.
4. Охарактеризуйте основные наиболее распространенные способы нарушения информационной безопасности
5. Охарактеризуйте процесс обеспечения собственной информационной безопасности на предприятиях.
6. Укажите основные международные организации, действующие в сфере информационной безопасности и укажите решаемые ими задачи.
7. Опишите отличительные особенности крупных международных профессиональных (отраслевых) организаций (объединений).
8. Дайте определение системы управления информационной безопасностью (СУИБ) предприятия, приведите её состав и цели создания.
9. Основные этапы и условия разработки СУИБ.
10. Опишите организационную структуру менеджмента обеспечения информационной безопасности предприятия
11. Основные функции отдела информационной безопасности предприятия.
12. Сценарий анализа информационных рисков компании
13. Дайте определение и поясните смысл политики безопасности предприятия
14. Поясните основные этапы управления безопасностью информационных технологий.
15. Опишите процедуру оценки общего уровня риска при управлении безопасностью информационных технологий.
16. Дайте определение и раскройте задачи, решаемые департаментом информационной безопасности предприятия (ДИБП).
17. Опишите функции ДИБП, связанные с формированием, поддержкой и документальным обеспечением политики информационной безопасности предприятия.
18. Опишите функции ДИБП, с внедрением средств защиты информации.
19. Опишите функции ДИБП, связанные с администрированием информационных систем и систем защиты информации

20. Дайте определение аудита состояния информационной безопасности предприятия. Охарактеризуйте их виды.
21. Опишите цели и стратегическую задачу аудита состояния информационной безопасности предприятия.
22. Опишите требования к организациям, осуществляющим внешний аудит состояния информационной безопасности предприятия.
23. Основные этапы аудита состояния информационной безопасности предприятия и их характеристика
24. Охарактеризуйте процесс анализа действующей на предприятии политики безопасности.
25. Охарактеризуйте процесс изучения (проверки) действующих информационных ресурсов предприятия.
26. Виды программных средств поддержки реализации политики информационной безопасности.
27. Структура и краткое содержание отчета о состоянии информационной безопасности программного продукта «COBRA».
28. Дайте характеристику программного комплекса управления политикой информационной безопасности компании «КОНДОР+».
29. Предпосылки разработки политики безопасности предприятия.
30. Структура деятельности в сфере информационной безопасности. Основные задачи организационно-управленческой деятельности (менеджмента) в сфере информационной безопасности
31. Что включает в себя безопасная информационная инфраструктура?
32. Иерархия уровней организационной работы в сфере информационной безопасности и их характеристика
33. Охарактеризуйте этап разработки СУИБ: Оценка информационных рисков
34. Охарактеризуйте этап разработки СУИБ: Внедрение выбранных мер обработки рисков
35. Охарактеризуйте этап разработки СУИБ: Контроль выполнения и эффективности выбранных мер.
36. Охарактеризуйте верхний уровень политики информационной безопасности предприятия
37. Охарактеризуйте средний уровень политики информационной безопасности предприятия
38. Приведите перечень основных вопросов, входящих в состав политики безопасности информационных технологий.
39. Опишите функции ДИБП, связанные с контролем выполнения требований политики информационной безопасности и проведением аудитов.
40. Инструментальная проверка защищенности информационной системы предприятия.
41. Анализ собранной информации при аудите состояния информационной безопасности предприятия.
42. Содержание заключения при аудите состояния информационной безопасности предприятия.
43. Назначение программных средства, реализующих методологии анализа рисков.
44. Опишите назначение и возможности семейства программных продуктов "CRAMM".
45. Назначение и основные функции программных средств, интегрируемых в информационную систему предприятия.
46. Перечислите и охарактеризуйте известные программные средства, интегрируемые в информационную систему предприятия.

47. Дайте характеристику услуги первичной постановки системы управления информационной безопасностью.
48. Страхование в сфере информационной безопасности и основные объекты страхования.
49. Общая политика России в сфере информационной безопасности
50. Структура органов государственной власти, обеспечивающих информационную безопасность в РФ.

Образец билета к зачету:

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Грозненский государственный нефтяной технический университет им. акад. М.Д. Миллионщикова
Кафедра «ИВТ»
Дисциплина «Управление персоналом при обеспечении информационной безопасности»
Группа: **Семестр:**

Билет 1

1. Охарактеризуйте этап разработки СУИБ: Оценка информационных рисков
2. Охарактеризуйте основные наиболее распространенные способы нарушения информационной безопасности
3. Структура органов государственной власти, обеспечивающих информационную безопасность в РФ.

Преподаватель _____ **М.З. Исаева**
Зав.кафедрой _____ **Э.Д.Алисултанова**

7.3. Текущий контроль

Образец типового задания для лабораторных занятий

Лабораторная работа №2. НОРМАТИВНО-ПРАВОВЫЕ ДОКУМЕНТЫ И СТАНДАРТЫ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цель работы: знакомиться с нормативно-правовыми документами и стандартами в области защиты информации и информационной безопасности. Для проведения лабораторной работы используется следующее обеспечение: персональный компьютер, подключённый к Интернету.

Порядок выполнения работы Практическая работа содержит отчет. Отчет должен содержать:

1. название и цель работы;
2. формулировки практических упражнений;
3. заполнение таблицы;
4. вывод к практической работе;

5. ответы на контрольные вопросы.

Задание

1.Провести сравнение стандартов: «Руководящие документы ГТК» и «Единые критерии безопасности информационных технологий».

2.Ознакомиться с нормативно-правовыми документами и стандартами в области криптографии и шифрования.

3.Заполнить в таблице 4 «Криптографическое закрытие информации» столбец «Способ реализации», указав способ реализации: аппаратный, программный или аппаратно-программный.

Таблица 4. Криптографическое закрытие информации

Вид преобразований	Способ преобразования	Разновидность способа	Способ реализации
Шифрование	Замена	Простая (одноалфавитная)	
	(подстановка)		
		Многоалфавитная	
		одноконтурная обыкновенна	
		Многоалфавитная	
		одноконтурная	
		монофоническая	
		Многоалфавитная	
		многоконтурная	
	Перестановка	Простая	
		Усложненная по таблице	
		Усложненная по маршрутам	
	Аналитическое	По правилам алгебры матриц	
	преобразование	По особым зависимостям	
	Гаммирование	С конечной короткой гаммой	
		С конечной динной гаммой	
		С бесконечной гаммой	
	Комбинированные	Замена+перестановка	
		Замена+гаммирование	
		Перестановка+	
		гаммирование	
		Гаммрование+гаммирование	
Кодирование	Смысловое	По специальным таблицам	
		(словарям)	
	Символьное	По кодовому алфавиту	
Другие виды	Рассечение-	Смысловое	
	разнесение		
		Механическое	
	Сжатие-		
	расширение		

Таблицу сохранить в отчёте.

1. Сравнить алгоритмы шифрования: хэширования, цифровой подписи по размеру ключа, размеру файла, скорости работы.

2. Определите время перебора всех паролей, состоящих из 6 цифр при скорости перебора 10 паролей в секунду.

3. Определите минимальную длину пароля, алфавит которого состоит из 10 символов, время перебора которого было не меньше 10 лет при скорости перебора 10 паролей в секунду.

Выводы_____
_____
_____
_____
_____

Контрольные вопросы

1. Охарактеризуйте симметричные алгоритмы шифрования.
2. В чём отличие потоковых и блочных шифров.
3. Перечислите требования к выбору и использованию паролей.
4. Перечислите и охарактеризуйте основные типы политики безопасности.

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-2. Способен выполнять работы по установке, настройке и техническому обслуживанию защищенных технических средств обработки информации					
Знать: технические описания и инструкции по эксплуатации технических средств обработки информации в защищенном исполнении, методы контроля защищенности информации от несанкционированного доступа и специальных программных воздействий, порядок аттестации объектов информатизации на соответствие требованиям безопасности информации	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	Билеты к зачету, текущий контроль
Уметь: проводить настройку защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами, Проводить техническое обслуживание защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-технической	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть: методами защиты информации от несанкционированного доступа и специальных программных воздействий на нее	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	

ПК-3. Способен осуществлять аудит защищенности информации в автоматизированных системах					
Знать: методы контроля эффективности защиты информации от несанкционированного доступа и утечки по техническим каналам; принципы построения систем защиты информации; организационные меры по защите информации	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	Билеты к зачету, текущий контроль
Уметь: разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем; применять инструментальные средства контроля защищенности информации в автоматизированных системах	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть: методами оценки информационных рисков безопасности информации в автоматизированной системе.	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

9.1 Литература

1. Мартынов А.П. Информационная безопасность и защита информации : учебное пособие / Мартынов А.П., Мартынова И.А., Русаков А.А.. — Москва : Ай Пи Ар Медиа, 2023. — 122 с. — ISBN 978-5-4497-2247-8. — Текст : электронный // IPR SMART : [сайт]. — URL:

https://www.iprbookshop.ru/131797.html (дата обращения: 02.09.2023). — Режим доступа: для авторизир. пользователей. - DOI: https://doi.org/10.23682/131797\

2. Программно-аппаратные средства защиты информации : учебное пособие для студентов вузов по направлению подготовки «Информационная безопасность» / Л.Х. Мифтахова [и др.].. — Санкт-Петербург : Интермедия, 2018. — 408 с. — ISBN 978-5-4383-0157-8. — Текст : электронный // IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/73644.html (дата обращения: 02.09.2023). — Режим доступа: для авторизир. Пользователей

3. Капгер, И. В. Управление информационной безопасностью : учебное пособие / И. В. Капгер, А. С. Шабуров. — Пермь :ПНИПУ, 2023. — 91 с. — ISBN 978-5-398-02866-9. — Текст :электронный // Лань : электронно-библиотечная система. —URL: https://e.lanbook.com/book/328889 — Режим доступа: для авториз. пользователей.

4. Мошак, Н. Н. Основы управления информационной безопасностью : учебное пособие / Н. Н. Мошак ; под редакцией В.В. Овчинникова. — Санкт-Петербург : ГУАП, 2022. — 141 с. — ISBN 978-5-8088-1711-1. — Текст : электронный // Лань :электронно-библиотечная система. — URL: https://e.lanbook.com/book/340967 — Режим доступа: для авториз. пользователей

9.2. Методические указания по освоению дисциплины «Управление персоналом при обеспечении информационной безопасности». (Приложение)

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.

Приложение

Методические указания по освоению дисциплины

«*Управление персоналом при обеспечении информационной безопасности*»

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 «Управление персоналом при обеспечении информационной безопасности» 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 дополнительныйматериал 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 особоевнимание 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 кконкретной 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 «Управление персоналом при обеспечении 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, уточнятьи 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.

Составитель:

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

СОГЛАСОВАНО:
Зав. выпускающей кафедрой
«Информатика и вычислительная техника» /Э.Д. Алисултанова/

Директор ДУМР / М.А. Магомаева /