МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "ДОНЕЦКАЯ АКАДЕМИЯ УПРАВЛЕНИЯ И ГОСУДАРСТВЕННОЙ СЛУЖБЫ"

Факультет **Факультет государственной службы и управления**

Кафедра **Информационных технологий**

"УТВЕРЖДАЮ"
Проректор
_____Л.Н. Костина
27.04.2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.05 Защита информации в корпоративных информационных системах"

Направление подготовки 09.04.03 Прикладная информатика
Профиль "Корпоративные информационные системы"

Квалификация ***МАГИСТР***

Форма обучения ***очная***

Общая трудоемкость ***5 ЗЕТ***

Год начала подготовки по учебному плану ***2024***

Донецк
2024

Составитель(и):
канд. экон. наук, доцент _____Н.Э. Тарусина

Рецензент(ы):
канд. экон. наук, доцент _____И.В. Стешенко

Рабочая программа дисциплины (модуля) " Защита информации в корпоративных информационных системах" разработана в соответствии с:

Федеральным государственным образовательным стандартом высшего образования - магистратура по направлению подготовки 09.04.03 Прикладная информатика (приказ Минобрнауки России от 19.09.2017 г. № 916)

Рабочая программа дисциплины (модуля) составлена на основании учебного плана Направление подготовки 09.04.03 Прикладная информатика
Профиль "Корпоративные информационные системы", утвержденного Ученым советом ФГБОУ ВО "ДОНАУИГС" от 27.04.2024 протокол № 12.

Срок действия программы: 2024-2026

Рабочая программа рассмотрена и одобрена на заседании кафедры Информационных технологий

Протокол от 16.04.2024 № 9

Заведующий кафедрой:
канд. физ.-мат. наук, доцент Брадул Н.В. _____
(подпись)

Визирование РПД для исполнения в очередном учебном году

"УТВЕРЖДАЮ"

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2025 - 2026 учебном году на заседании кафедры Информационных технологий

Протокол от "____" _____ 2025 г. №__

Зав. кафедрой канд. физ.-мат. наук, доцент Брадул Н.В. _____ (подпись)

Визирование РПД для исполнения в очередном учебном году

"УТВЕРЖДАЮ"

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2026 - 2027 учебном году на заседании кафедры Информационных технологий

Протокол от "____" _____ 2026 г. №__

Зав. кафедрой канд. физ.-мат. наук, доцент Брадул Н.В. _____ (подпись)

Визирование РПД для исполнения в очередном учебном году

"УТВЕРЖДАЮ"

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2027 - 2028 учебном году на заседании кафедры Информационных технологий

Протокол от "____" _____ 2027 г. №__

Зав. кафедрой канд. физ.-мат. наук, доцент Брадул Н.В. _____ (подпись)

Визирование РПД для исполнения в очередном учебном году

"УТВЕРЖДАЮ"

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2028 - 2029 учебном году на заседании кафедры Информационных технологий

Протокол от "____" _____ 2028 г. №__

Зав. кафедрой канд. физ.-мат. наук, доцент Брадул Н.В. _____ (подпись)

РАЗДЕЛ 1. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ

1.1. ЦЕЛИ ДИСЦИПЛИНЫ

Цель освоения дисциплины – формирование компетенций магистров в области аудита состояния информационной безопасности корпоративных информационных систем.

1.2. УЧЕБНЫЕ ЗАДАЧИ ДИСЦИПЛИНЫ

Задачи учебной дисциплины:
- ознакомится с законодательным уровнем обеспечения информационной безопасности;
- изучить административный уровень информационной безопасности;
- научиться использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации ИС.

1.3.2. Дисциплина " Защита информации в корпоративных информационных системах" выступает опорой для следующих элементов:

Преддипломная практика

1.4. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ:

ПК-5.1: Анализирует угрозы информационной безопасности корпоративных информационных систем, применяет комплексный подход к обеспечению информационной безопасности корпоративных систем

Знать:

Уровень 1	основные понятия защиты информации и политики безопасности, структуру системы защиты информации в корпоративных информационных системах
Уровень 2	методы защиты корпоративной информации
Уровень 3	международные и отечественные стандарты информационной безопасности

Уметь:

Уровень 1	анализировать угрозы информационной безопасности корпоративных информационных систем
Уровень 2	выбирать методы и алгоритмы защиты корпоративной информации
Уровень 3	учитывать международные и отечественные стандарты информационной безопасности в профессиональной деятельности

Владеть:

Уровень 1	навыками анализа угроз информационной безопасности корпоративных информационных систем
Уровень 2	методами и алгоритмами защиты корпоративной информации
Уровень 3	навыками комплексного подхода к обеспечению информационной безопасности корпоративных систем

В результате освоения дисциплины " Защита информации в корпоративных

3.1	**Знать:**
	базовые понятия и принципы политики безопасности, законодательный уровень обеспечения информационной безопасности.
3.2	**Уметь:**
	использовать комплексный подход к обеспечению информационной безопасности корпоративных систем
3.3	**Владеть:**
	методами и средствами защиты от вредоносных программ, методами обнаружения и предотвращения вторжений в корпоративные информационные системы; передовыми
	методами оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации ИС

1.5. ФОРМЫ КОНТРОЛЯ

Текущий контроль успеваемости позволяет оценить уровень сформированности элементов компетенций (знаний, умений и приобретенных навыков), компетенций с последующим объединением оценок и проводится в форме: устного опроса на лекционных и семинарских/практических занятиях (фронтальный, индивидуальный, комплексный), письменной проверки (тестовые задания, контроль знаний по разделу, ситуационных заданий и т.п.), оценки активности работы обучающегося на занятии, включая задания для самостоятельной работы.

Промежуточная аттестация

Результаты текущего контроля и промежуточной аттестации формируют рейтинговую оценку работы студента. Распределение баллов при формировании рейтинговой оценки работы студента осуществляется в соответствии с действующим локальным нормативным актом. По дисциплине " Защита информации в корпоративных информационных системах" видом промежуточной аттестации является Экзамен

РАЗДЕЛ 2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. ТРУДОЕМКОСТЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Общая трудоёмкость дисциплины " Защита информации в корпоративных информационных системах" составляет 5 зачётные единицы, 180 часов.

Количество часов, выделяемых на контактную работу с преподавателем и самостоятельную работу обучающегося, определяется учебным планом.

2.2. СОДЕРЖАНИЕ РАЗДЕЛОВ ДИСЦИПЛИНЫ

Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Примечание
Раздел 1. Проблемы безопасности корпоративной информации. Технологии защиты корпоративных данных						
Тема 1.1. Основные понятия и анализ угроз /Лек/	2	2	ПК-5.1	Л1.1 Л1.2Л2.1Л3 .1 Л3.2 Л3.3 Э1 Э3	0	
Тема 1.1. Основные понятия и анализ угроз /Пр/	2	1	ПК-5.1	Л1.1 Л1.2Л2.1Л3 .1 Л3.2 Л3.3 Э1 Э3	0	
Тема 1.1. Основные понятия и анализ угроз /Ср/	2	6	ПК-5.1	Л1.1 Л1.2Л2.1Л3 .1 Л3.2 Л3.3 Э1 Э3	0	
Тема 1.2. Политика информационной безопасности /Лек/	2	2	ПК-5.1	Л1.1 Л1.2Л2.1Л3 .1 Л3.2 Л3.3 Э1 Э3	0	
Тема 1.2. Политика информационной безопасности /Пр/	2	1	ПК-5.1	Л1.1 Л1.2Л2.1Л3 .1 Л3.2 Л3.3 Э1 Э3	0	
Тема 1.2. Политика информационной безопасности /Ср/	2	6	ПК-5.1	Л1.1 Л1.2Л2.1Л3 .1 Л3.2 Л3.3 Э1 Э3	0	
Тема 1.3. Криптографическая защита информации /Лек/	2	4	ПК-5.1	Л1.1 Л1.2Л2.1Л3 .1 Л3.2 Л3.3 Э1 Э3	0	
Тема 1.3. Криптографическая защита	2	2	ПК-5.1	Л1.1	0	

информации /Пр/				Л1.2Л2.1Л3.1 Л3.2 Л3.3 Э1 Э3		
Тема 1.3. Криптографическая защита информации /Ср/	2	6	ПК-5.1	Л1.1 Л1.2Л2.1Л3.1 Л3.2 Л3.3 Э1 Э3	0	
Тема 1.4. Идентификация, аутентификация и управление доступом /Лек/	2	2	ПК-5.1	Л1.1 Л1.2Л2.1Л3.1 Л3.2 Л3.3 Э1 Э3	0	
Тема 1.4. Идентификация, аутентификация и управление доступом /Пр/	2	0	ПК-5.1	Л1.1 Л1.2Л2.1Л3.1 Л3.2 Л3.3 Э1 Э3	0	
Тема 1.4. Идентификация, аутентификация и управление доступом /Ср/	2	6	ПК-5.1	Л1.1 Л1.2Л2.1Л3.1 Л3.2 Л3.3 Э1 Э3	0	
Тема 1.5. Защита электронного документооборота /Лек/	2	2	ПК-5.1	Л1.1 Л1.2Л2.1Л3.1 Л3.2 Л3.3 Э3	0	
Тема 1.5. Защита электронного документооборота /Пр/	2	2	ПК-5.1	Л1.1 Л1.2Л2.1Л3.1 Л3.2 Л3.3 Э3	0	
Тема 1.5. Защита электронного документооборота /Ср/	2	8	ПК-5.1	Л1.1 Л1.2Л2.1Л3.1 Л3.2 Л3.3 Э3	0	
Раздел 2. Комплексная защита корпоративных информационных систем						
Тема 2.1. Принципы комплексной защиты информации КИС /Лек/	2	2	ПК-5.1	Л1.1 Л1.2Л2.1Л3.1 Л3.2 Л3.3 Э2 Э3	0	
Тема 2.1. Принципы комплексной защиты информации КИС /Пр/	2	2	ПК-5.1	Л1.1 Л1.2Л2.1Л3.1 Л3.2 Л3.3 Э2 Э3	0	
Тема 2.1. Принципы комплексной защиты информации КИС /Ср/	2	6	ПК-5.1	Л1.1 Л1.2Л2.1Л3.1 Л3.2 Л3.3	0	

				Э2 Э3		
Тема 2.2 Защита от вредоносных программ /Лек/	2	4	ПК-5.1	Л1.1 Л1.2Л2.1Л3.1 Л3.2 Л3.3 Э2 Э3	0	
Тема 2.2 Защита от вредоносных программ /Пр/	2	2	ПК-5.1	Л1.1 Л1.2Л2.1Л3.1 Л3.2 Л3.3 Э2 Э3	0	
Тема 2.2 Защита от вредоносных программ /Ср/	2	8	ПК-5.1	Л1.1 Л1.2Л2.1Л3.1 Л3.2 Л3.3 Э2 Э3	0	
Тема 2.3 Обнаружение и предотвращение вторжений /Лек/	2	4	ПК-5.1	Л1.1 Л1.2Л2.1Л3.1 Л3.2 Л3.3 Э2 Э3	0	
Тема 2.3 Обнаружение и предотвращение вторжений /Пр/	2	2	ПК-5.1	Л1.1 Л1.2Л2.1Л3.1 Л3.2 Л3.3 Э2 Э3	0	
Тема 2.3 Обнаружение и предотвращение вторжений /Ср/	2	8	ПК-5.1	Л1.1 Л1.2Л2.1Л3.1 Л3.2 Л3.3 Э2 Э3	0	
Тема 2.4 Межсетевое экранирование /Лек/	2	2	ПК-5.1	Л1.1 Л1.2Л2.1Л3.1 Л3.2 Л3.3 Э3	0	
Тема 2.4 Межсетевое экранирование /Пр/	2	1	ПК-5.1	Л1.1 Л1.2Л2.1Л3.1 Л3.2 Л3.3 Э3	0	
Тема 2.4 Межсетевое экранирование /Ср/	2	8	ПК-5.1	Л1.1 Л1.2Л2.1Л3.1 Л3.2 Л3.3 Э3	0	
Тема 2.5 Виртуальные защищенные сети VPN /Лек/	2	2	ПК-5.1	Л1.1 Л1.2Л2.1Л3.1 Л3.2 Л3.3 Э3	0	
Тема 2.5 Виртуальные защищенные сети VPN /Пр/	2	1	ПК-5.1	Л1.1 Л1.2Л2.1Л3.1 Л3.2 Л3.3 Э3	0	
Тема 2.5 Виртуальные защищенные сети VPN /Ср/	2	8	ПК-5.1	Л1.1 Л1.2Л2.1Л3	0	

				.1 Л3.2 Л3.3 Э3		
Раздел 3. Управление информационной безопасностью						
Тема 3.1 Управление средствами обеспечения информационной безопасности /Лек/	2	4	ПК-5.1	Л1.1 Л1.2Л2.1Л3 .1 Л3.2 Л3.3 Э2 Э3	0	
Тема 3.1 Управление средствами обеспечения информационной безопасности /Пр/	2	1	ПК-5.1	Л1.1 Л1.2Л2.1Л3 .1 Л3.2 Л3.3 Э2 Э3	0	
Тема 3.1 Управление средствами обеспечения информационной безопасности /Ср/	2	16	ПК-5.1	Л1.1 Л1.2Л2.1Л3 .1 Л3.2 Л3.3 Э2 Э3	0	
Тема 3.2 Стандарты информационной безопасности /Лек/	2	2	ПК-5.1	Л1.1 Л1.2Л2.1Л3 .1 Л3.2 Л3.3 Э2 Э3	0	
Тема 3.2 Стандарты информационной безопасности /Пр/	2	1	ПК-5.1	Л1.1 Л1.2Л2.1Л3 .1 Л3.2 Л3.3 Э2 Э3	0	
Тема 3.2 Стандарты информационной безопасности /Ср/	2	17	ПК-5.1	Л1.1 Л1.2Л2.1Л3 .1 Л3.2 Л3.3 Э2 Э3	0	
/Конс/	2	2			0	

РАЗДЕЛ 3. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В процессе освоения дисциплины используются следующие образовательные технологии: лекции (Л), практические занятия (ПР), самостоятельная работа студентов (СР) по выполнению различных видов заданий.

1. В процессе освоения дисциплины используются следующие интерактивные образовательные технологии: Лекционный материал представлен в виде слайд-презентации в формате «Power Point». Для наглядности используются материалы различных справочных материалов, научных статей т.д. В ходе лекции предусмотрена обратная связь со студентами, активизирующие вопросы, просмотр и обсуждение видеофильмов. При проведении лекций используется проблемно-ориентированный междисциплинарный подход, предполагающий творческие вопросы и создание дискуссионных ситуаций.

2. При изложении теоретического материала используются такие методы:

− монологический;
− показательный;
− диалогический;

− эвристический;
− исследовательский.
3. Используются следующие принципы дидактики высшей школы:
− последовательность обучения;
− систематичность обучения;
− доступность обучения;
− принцип научности;
− принципы взаимосвязи теории и практики;
− принцип наглядности и др.
В конце каждой лекции предусмотрено время для ответов на проблемные вопросы.
4. Самостоятельная работа предназначена для внеаудиторной работы студентов, связанной с изучением дополнительной литературы по дисциплине, подготовкой к текущему и семестровому контролю, а также выполнением индивидуального задания за компьютером с использованием необходимого программного обеспечения, в форме реферата, презентации.

РАЗДЕЛ 4. УЧЕБНО-МЕТОДИЧЕСКОЕ И МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

4.1. Рекомендуемая литература

1. Основная литература

	Авторы,	Заглавие	Издательство, год
Л1.1	А. А. Внуков	Защита информации в банковских системах: учебное пособие для вузов (246 с.)	Москва: Издательство Юрайт, 2021
Л1.2	В. А. Астапчук, П. В. Терещенко	Корпоративные информационные системы: требования при проектировании: учебное пособие для вузов / — 2-е изд., испр. и доп. (113 с.)	Москва: Издательство Юрайт, 2022

2. Дополнительная литература

	Авторы,	Заглавие	Издательство, год
Л2.1	Н. Г. Чиркина	Информационные системы и технологии: учебное пособие (146 с.)	Екатеринбург: УрГЭУ, 2018

3. Методические разработки

	Авторы,	Заглавие	Издательство, год
Л3.1	Н.Э. Тарусина	Конспект лекций по учебной дисциплине «Защита информации в корпоративных информационных системах» для обучающихся 1 курса образовательной программы магистратуры направления подготовки 09.04.03 «Прикладная информатика» очной / заочной форм обучения (192 с.)	Донецк : ДОНАУИГС, 2022
Л3.2	Н.Э. Тарусина	Методические рекомендации для проведения практических занятий по учебной дисциплине «Защита информации в корпоративных информационных системах» для обучающихся 1 курса образовательной программы магистратуры направления подготовки 09.04.03 «Прикладная информатика» очной / заочной форм обучения (21 с.)	Донецк : ДОНАУИГС, 2022
Л3.3	Н. Э. Тарусина	Защита информации в корпоративных информационных системах : методические рекомендации по организации самостоятельной работы для обучающихся 1 курса образовательной программы магистратуры направления подготовки 09.04.03 Прикладная информатика очной / заочной форм обучения (65 с.)	Донецк :ДОНАУИГС, 2022

4.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Научная электронная библиотека «КиберЛенинка»	https://cyberleninka.ru/
Э2	Образовательная платформа Юрайт	https://urait.ru

Э3	Библиотека ФГБОУ ВО «ДОНЕЦКАЯ АКАДЕМИЯ УПРАВЛЕНИЯ И ГОСУДАРСТВЕННОЙ СЛУЖБЫ»	https://donampa.ru/biblioteka

4.3. Перечень программного обеспечения

Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства:
При проведении лекций используется аудитория с мультимедийным оборудованием. Аудиторные занятия проводятся в компьютерных классах с доступом к сети Интернет. Для проведения консультаций в online-режиме используется LMS Moodle, Telemost.yandex.ru, видеозвонки Mail.ru. Программное обеспечение: операционная система Windows XP и выше, пакет Microsoft Office 2010 и выше.

4.4. Профессиональные базы данных и информационные справочные системы

Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду (ЭИОС ГОУ ВПО ДОНАУИГС) и электронно-библиотечную систему (ЭБС IPRbooks), а также возможностью индивидуального неограниченного доступа обучающихся в ЭБС и ЭИОС посредством Wi-Fi с персональных мобильных устройств.

4.5. Материально-техническое обеспечение дисциплины

1. Учебная аудитория для проведения занятий лекционного, семинарского типа, групповых занятий и консультаций, текущего контроля и промежуточной аттестации: аудитория № 808 учебный корпус № 1.
- компьютеры (12); программное обеспечение - Microsoft Office 2010 (лицензия № 47556582 от 19.10.2010 г., лицензия № 49048130 от 19.09.2011);
- специализированная мебель: рабочее место преподавателя, рабочие места обучающихся (26), стационарная доска.
2. Помещения для самостоятельной работы с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно образовательную среду организации:
читальные залы, учебные корпуса 1, 6. Адрес: г. Донецк, ул. Челюскинцев 163а, г. Донецк, ул. Артема 94.
Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду (ЭИОС ГОУ ВПО ДОНАУИГС) и электронно-библиотечную систему (ЭБС IPRbooks), а также возможностью индивидуального неограниченного доступа обучающихся в ЭБС и ЭИОС посредством Wi-Fi с персональных мобильных устройств.
Сервер: AMD FX 8320/32Gb(4x8Gb)/4Tb(2x2Tb). На сервере установлена свободно распространяемая операционная система DEBIAN 10. MS Windows 8.1 (Лицензионная версия операционной системы подтверждена сертификатами подлинности системы Windows на корпусе ПК), MS Windows XP (Лицензионная версия операционной системы подтверждена сертификатами подлинности системы Windows на корпусе ПК), MS Windows 7 (Лицензионная версия операционной системы подтверждена сертификатами подлинности системы Windows на корпусе ПК), MS Office 2007 Russian OLP NL AE (лицензии Microsoft № 42638778, № 44250460), MS Office 2010 Russian (лицензии Microsoft № 47556582, № 49048130), MS Office 2013 Russian (лицензии Microsoft № 61536955, № 62509303, № 61787009, № 63397364), Grub loader for ALT Linux (лицензия GNU LGPL v3), Mozilla Firefox (лицензия MPL2.0), Moodle (Modular Object-Oriented Dynamic Learning Environment, лицензия GNU GPL), IncScape (лицензия GPL 3.0+), PhotoScape (лицензия GNU GPL), 1С ERP УП, 1С ЗУП (бесплатные облачные решения для образовательных учреждений от 1Cfresh.com), OnlyOffice 10.0.1 (SaaS, GNU Affero General Public License3).

РАЗДЕЛ 5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания

ВОПРОСЫ К ЭКЗАМЕНУ ПО РАЗДЕЛАМ (ТЕМАМ) ДИСЦИПЛИНЫ (МОДУЛЯ)

1. Сформулируйте понятие информационной безопасности ИС.
2. Объясните понятия целостности, конфиденциальности и доступности информации.
3. Объясните понятия идентификации, аутентификации и авторизации пользователя. Как они взаимосвязаны?
4. Укажите отличия санкционированного доступа от несанкционированного доступа к информации.
5. Сформулируйте определение политики безопасности.
6. Сформулируйте особенности избирательной и полномочной политики безопасности.
7. Объясните понятие «угроза безопасности ИС».
8. Укажите основные признаки классификации возможных угроз безопасности ИС.
9. Каковы основные виды угроз безопасности ИС по цели и степени воздействия?
10. Дайте краткую характеристику угроз безопасности, обозначаемых терминами: «троянский конь»,
11. «вирус», «червь»?
12. Перечислите и дайте краткую характеристику основных методов реализации угроз информационной безопасности.
13. Объясните суть комплексного подхода к обеспечению информационной безопасности ИС.

14. Объясните понятие «политика безопасности организации».
15. Какие разделы должна содержать документально оформленная политика безопасности?
16. Какие проблемы решает верхний уровень политики безопасности?
17. Какие задачи решает средний уровень политики безопасности?
18. Каковы особенности нижнего уровня политики безопасности?
19. Сформулируйте обязанности руководителей подразделений, администраторов и пользователей при реализации политики безопасности.
20. Опишите структуру политики безопасности организации.
21. Что представляют собой специализированные политики безопасности?
22. Приведите несколько примеров специализированных политик безопасности с описанием их особенностей.
23. Что представляют собой процедуры безопасности?
24. Приведите несколько примеров процедур безопасности с описанием их особенностей.
25. Сформулируйте основные этапы разработки политики безопасности организации.
26. Что такое криптография?
27. Дайте определения следующих понятий: криптограмма, криптоалгоритм, криптосистема.
28. В чем состоит коренное различие симметричных и асимметричных криптосистем?
29. Охарактеризуйте четыре основных режима работы блочного алгоритма.
30. Расскажите о способах комбинирования блочных алгоритмов для получения алгоритмов с более длинным ключом, сравните их между собой.
31. Каковы основные характеристики и режимы работы отечественного стандарта шифрования данных?
32. Сформулируйте концепцию криптосистемы с открытым ключом?
33. Дайте определение однонаправленной функции. Приведите примеры однонаправленных функций.
34. Каковы особенности однонаправленных функций с «потайным ходом»?
35. На чем основывается надежность криптоалгоритма шифрования RSA?
36. Опишите две основные процедуры, осуществляемые системой электронной цифровой подписи для подтверждения подлинности электронного документа.
37. Опишите отечественный стандарт цифровой подписи, укажите его преимущества по сравнению с алгоритмом цифровой подписи DSA.
38. Каково назначение хэш-функции и каким требованиям должна удовлетворять качественная хэш-функция?
39. Каким образом комбинированный метод шифрования позволяет сочетать достоинства асимметричных и симметричных криптосистем? Опишите протокол реализации комбинированного метода шифрования.
40. Опишите работу алгоритма Диффи - Хэллмана. Укажите достоинства этого алгоритма.
41. Каково назначение инфраструктуры открытых ключей PKI? Опишите функционирование инфраструктуры PKI.
42. Дайте определения понятий: идентификация, аутентификация, авторизация, администрирование. Что понимают под решением задач AAA?
43. Какие задачи решает подсистема управления идентификацией и доступом IAM (Identity and Access Management)?
44. На какие категории можно разделить процессы аутентификации в зависимости от сущностей, предъявляемых пользователем для подтверждения своей подлинности?
45. Перечислите основные атаки на протоколы аутентификации.
46. Опишите метод аутентификации на основе многоразовых паролей. Каковы недостатки этого метода?
47. Опишите метод аутентификации на основе одноразовых паролей. Каковы его достоинства и недостатки?
48. Сформулируйте принцип строгой аутентификации. Опишите типы процедур строгой аутентификации.
49. Объясните назначение PIN-кода и особенности его использования.
50. Объясните принцип работы двухфакторной аутентификации. Какие внешние носители информации используются для двухфакторной аутентификации пользователей? Каковы достоинства этого метода аутентификации?
51. Опишите функциональность и характеристики смарт-карт и USB-токенов.
52. Опишите методы биометрической аутентификации пользователя. Что означают коэффициент ошибочных отказов и коэффициент ошибочных подтверждений?
53. Поясните принцип управления доступом по схеме однократного входа с авторизацией Single Sign-On.
54. Укажите особенности построения и функционирования системы распределенного электронного документооборота.

55. Назовите угрозы информационной безопасности для СЭД и охарактеризуйте источники этих угроз.
56. Какие функции должны быть реализованы средствами защиты информации СЭД?
57. Сформулируйте основополагающие принципы построения современных КИС.
58. Охарактеризуйте четыре уровня управления КИС.
59. Укажите необходимые условия обеспечения санкционированного доступа к информационным ресурсам предприятия.
60. Какие важные системные функции может выполнять КИС при реализации в ней принципа централизованного управления?
61. Объясните значение управления рисками предприятия для создания системы эффективной защиты информации на этом предприятии.
62. Какие требования необходимо учитывать при разработке архитектуры КСЗИ?
63. Перечислите меры и средства защиты, применяемые при построении комплексной системы защиты информации КИС.
64. Укажите основные подсистемы информационной безопасности, входящие в состав КСЗИ.
65. Опишите особенности подсистемы защиты информации от несанкционированного доступа.
66. Опишите назначение и особенности подсистемы контроля эффективности защиты информации.
67. Опишите назначение и особенности подсистемы мониторинга и управления инцидентами ИБ.
68. Опишите назначение и особенности подсистемы обеспечения непрерывности функционирования средств защиты.
69. Что такое вредоносная программа? Охарактеризуйте основные типы вредоносных программ.
70. Укажите существенные отличия компьютерных вирусов от сетевых «червей». Опишите основные особенности «троянских» программ.
71. Опишите два основных подхода к обнаружению вредоносных программ.
72. Как выполняется сигнатурный анализ? Каковы его достоинства и недостатки?
73. Что представляют собой проактивные методы обнаружения?
74. Опишите принцип действия, достоинства и недостатки эвристических анализаторов.
75. Опишите принцип действия, достоинства и недостатки поведенческих блокираторов.
76. Назовите и опишите дополнительные модули антивирусных средств.
77. Каковы дополнительные меры и средства защиты от вредоносных программ, расширяющие возможности антивирусных программ?
78. Опишите меры и средства защиты от спама (нежелательной корреспонденции).
79. Каковы особенности реализации подсистемы защиты корпоративной информации от вредоносных программ и вирусов?
80. Сформулируйте понятия: обнаружение вторжений и предотвращение вторжений.
81. Укажите четыре признака системы IPS, отличающие ее от системы IDS.
82. Дайте определения понятий: сетевая система NIPS (network-based IPS) и хостовая система HIPS (host- based IPS).
83. Сформулируйте назначение и особенности применения специализированных средств - сканеров уязвимости (vulnerability assessment).
84. Какие методы анализа событий используются в процессе выявления вторжений?
85. В чем суть метода обнаружения аномального поведения?
86. В чем суть метода обнаружения злоупотреблений?
87. Опишите функциональность средств предотвращения вторжений системного (хостового) уровня
88. HIPS (Host-based IPS).
89. Опишите функциональность средств предотвращения вторжений сетевого уровня NIPS (network-based IPS).
90. Сформулируйте подход к защите от распределенных атак типа «отказ в обслуживании» DDoS (Distributed Denial of Service).
91. Какими свойствами и функциями должна обладать современная IPS для успешного обнаружения и предотвращения вторжений?
92. Опишите структуру и функционирование подсистемы предотвращения вторжений в КИС.
93. Что такое виртуальные защищенные сети VPN (Virtual Private Network)?
94. Сформулируйте концепцию построения виртуальных защищенных сетей VPN.
95. Объясните понятия «виртуальный защищенный туннель», «туннелирование» и «инкапсуляция».
96. Дайте развернутые определения таких устройств VPN, как VPN-клиент, VPN-сервер и VPN-шлюз безопасности.
97. Поясните особенности структуры и функционирования двух основных схем виртуальных защищенных каналов.
98. Каковы функции инициатора туннеля и терминатора туннеля?
99. Какие методы используют для обеспечения безопасности сетей VPN?

100. Опишите классификацию сетей VPN по рабочему уровню модели взаимодействия открытых систем
101. OSI (Open Systems Interconnection).
102. Каковы основные варианты архитектуры сетей VPN? Дайте пояснение для каждого из трех основных вариантов.
103. Укажите основные виды технической реализации VPN и дайте пояснения для каждого из них.
104. Какие российские компании выпускают VPN-продукты в настоящее время?
105. Опишите возможности и основные характеристики семейства VPN-продуктов CSP VPN 3.0 российской компании «С-Терра СиЭсПи».
106. Назовите задачи системы управления информационной безопасностью КИС.
107. Как осуществляется управление учетными записями и правами доступа к рабочим станциям, серверам и другим активным устройствам КИС?
108. В чем суть концепции глобального управления безопасностью GSM (Global Security Management)?
109. Объясните понятия «глобальная и локальная политики безопасности».
110. Опишите функционирование системы управления информационной безопасностью GSM.
111. Как осуществляется защита ресурсов в системе управления информационной безопасностью GSM?
112. Как осуществляется управление средствами информационной безопасности масштаба предприятия в системе GSM?
113. Опишите централизованное управление безопасностью, реализованное в продуктах Застава.
114. Опишите возможности системы управления Cisco Security Manager и программно-аппаратного комплекса управления Cisco MARS.
115. Какие функции реализуют продукты IBM Tivoli для обеспечения информационной безопасности КИС?
116. Назовите основные продукты IBM Tivoli и опишите их возможности.
117. Какие задачи решает система управления безопасностью IBM Proventia Management SiteProtector?
118. Сформулируйте главную задачу стандартов информационной безопасности с позиций производителей и потребителей продуктов информационных технологий, а также специалистов по сертификации этих продуктов.
119. Назовите основные международные стандарты информационной безопасности.
120. Дайте краткую характеристику международного стандарта ISO/IEC 17799:2000 (BS 7799-1:2000).
121. Каковы основные особенности германского стандарта BSI «Руководство по защите информационных технологий для базового уровня защищенности»?
122. Опишите содержание и укажите значение международного стандарта ISO 15408 «Общие критерии безопасности информационных технологий.
123. Перечислите стандарты для беспроводных сетей и дайте их краткую характеристику.
124. Назовите стандарты информационной безопасности для Интернета.
125. Каковы назначение и особенности функционирования протокола SET (Security Electronics Transaction)?
126. Каковы назначение и функциональность протоколов SSL (Secure Socket Layer) и IPSec? В чем эти протоколы существенно различаются?
127. Каковы назначение и функциональность инфраструктуры управления открытыми ключами PKI?
128. Перечислите российские стандарты безопасности информационных технологий.
129. Каково назначение стандарта ГОСТ Р ИСО/МЭК 15408? Назовите и охарактеризуйте три основные части этого стандарта.

ТИПОВЫЕ ТЕСТОВЫЕ ЗАДАНИЯ
ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ
ЗАДАНИЯ ЗАКРЫТОГО ТИПА
Раздел 1. Проблемы безопасности корпоративной информации. Технологии защиты корпоративных данных

ВЫБЕРИТЕ ОДИН ВЕРНЫЙ ОТВЕТ / ВЫБЕРИТЕ НЕСКОЛЬКО ВЕРНЫХ ОТВЕТОВ*

Задание 1. Защита информации - это _____
A. деятельность по возврату похищенной ранее информации и восстановление ее целостности.
B. Деятельность по хранению информации на открытом носителе
C. Процесс передачи информации по открытым каналам связи
D. деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию

Задание 2. Объект защиты - это_____
A. сооружение, которое должно находится под защитой.

B. информация или носитель информации, или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.
C. Какое-либо доверенное лицо имеющее доступ к важной информации.
D. Учетная запись пользователя на предприятии.

Задание 3. _Аппаратные средства это - _____
A. компьютеры и их составные части.
B. обслуживающий персонал и пользователи.
C. субъект, в полном объеме реализующий полномочия владения,
D. техническое, программное средство, вещество и/или материал,
E. предназначенные или используемые для защиты информации.

Задание 4. программное обеспечение - это _____
A. приобретенные программы, исходные, объектные, загрузочные модули операционные системы и системные программы
B. Персонал обслуживающий компьютер
C. Устройство для корректной работы компьютера
D. машинные носители информации в виде внешних устройств компьютерных систем

Задание 5. Данные - это
A. это статус, предоставленный и определяющий требуемую степень их защиты
B. хранимые временно и постоянно, на магнитных носителях, печатные, архивы, системные журналы и т.д.
C. понимают активные компоненты системы, которые могут стать причиной потока информации от объекта к субъекту или изменения состояния системы
D. доступности и целостности информационных компонентов и ресурсов системы

Задание 6. Причинами случайных воздействий при эксплуатации ИС могут быть:
A. аварийные ситуации из-за стихийных бедствий и отключений электропитания;
B. отказы и сбои аппаратуры;
C. ошибки в работе обслуживающего персонала и пользователей;
D. угрозы с использованием стандартного пути доступа к ресурсам ИС, например незаконное получение паролей и других реквизитов разграничения доступа с последующей маскировкой под зарегистрированного пользователя

Задание 7. Гипотетическая модель потенциального нарушителя_____
A. квалификация нарушителя может быть на уровне разработчика данной системы;
B. нарушитель выберет наиболее слабое звено в защите.
C. ошибки в программном обеспечении
D. помехи в линиях связи из-за воздействий внешней среды

Задание 8. Для защиты от вредоносных программ необходимо применение ряда мер:
A. исключить несанкционированный доступ к исполняемым файлам;
B. средства защиты от вредоносных программ
C. физическая защита
D. создать замкнутую среду исполнения программ.

Задание 9. К комплексу организационных мер относятся следующие меры безопасности:
A. планирование восстановительных работ.
B. управление персоналом;
C. механизмы идентификации и аутентификации;
D. средства криптографии.

Задание 10 Фарминг - это
A. Вид мошенничества, ставящий целью получить персональные данные пользователей.
B. Добывание криптовалюты
C. является относительно новым видом интернет-мошенничества, цель которого получить идентификационные данные пользователей.
D. может создавать угрозу доступности информации, блокируя почтовые серверы, либо использоваться для распространения вредоносного программного обеспечения.

*(ответ – все ответы верны – быть не может)

5.2. Темы письменных работ

ТЕМЫ РЕФЕРАТОВ, ДОКЛАДОВ ДЛЯ ПРОВЕРКИ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИИ

1. Основные понятия и анализ угроз информационной безопасности.
2. Политики безопасности.
3. Криптографическая защита информации.
4. Идентификация, аутентификация и управление доступом.
5. Защита электронного документооборота.
6. Принципы комплексной защиты информации КИС.
7. Защита от вредоносных программ.
8. Обнаружение и предотвращение вторжений.
9. Межсетевое экранирование.
10. Виртуальные защищенные сети VPN.
11. Управление средствами обеспечения информационной безопасности.
12. Стандарты информационной безопасности.

5.3. Фонд оценочных средств

Фонд оценочных средств дисциплины " Защита информации в корпоративных информационных системах" разработан в соответствии с локальным нормативным актом ФГБОУ ВО "ДОНАУИГС".

Фонд оценочных средств дисциплины " Защита информации в корпоративных информационных системах" в полном объеме представлен в виде приложения к данному РПД.

5.4. Перечень видов оценочных средств

Индивидуальные задания
Устный опрос по изучаемой теме (проводится на практических занятиях)
Контроль знаний раздела учебной дисциплины (письменный опрос)
Реферат (самостоятельная работа)
Доклад с презентацией зачитываются на практических занятиях объемом не более 5-и минут (самостоятельная работа)
Тестовые задания
Научная составляющая

РАЗДЕЛ 6. СРЕДСТВА АДАПТАЦИИ ПРЕПОДАВАНИЯ ДИСЦИПЛИНЫ К ПОТРЕБНОСТЯМ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей:

1) с применением электронного обучения и дистанционных технологий.

2) с применением специального оборудования (техники) и программного обеспечения, имеющихся в ФГБОУ ВО "ДОНАУИГС".

В процессе обучения при необходимости для лиц с нарушениями зрения, слуха и опорно-двигательного аппарата предоставляются следующие условия:

- для лиц с нарушениями зрения: учебно-методические материалы в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); индивидуальные задания и консультации.

- для лиц с нарушениями слуха: учебно-методические материалы в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.

- для лиц с нарушениями опорно-двигательного аппарата: учебно-методические материалы в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

РАЗДЕЛ 7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО УСВОЕНИЮ ДИСЦИПЛИНЫ

Аудиторные занятия по дисциплине "Защита информации в корпоративных информационных системах" проводятся в форме лекционных и практических занятий.
На лекционных занятиях, согласно учебному плану дисциплины, обучающимся предлагается рассмотреть

основные темы курса. Студенту предлагается участвовать в диалоге с преподавателем, в ходе которого могут обсуждаться моменты, актуальные для его будущей практической деятельности; он может высказать свое мнение после сопоставления разных фактов и разнообразных точек зрения на них.
К числу важнейших умений, являющихся неотъемлемой частью успешного учебного процесса, относится умение работать с различными литературными источниками, содержание которых так или иначе связано с изучаемой дисциплиной.
Подготовку к любой теме курса рекомендуется начинать с изучения презентационных материалов или учебной литературы, в которых дается систематизированное изложение материала, разъясняется смысл разных терминов и сообщается об изменениях в подходах к изучению тех или иных проблем данного курса.
Методические указания по организации самостоятельной работы
Самостоятельная работа по дисциплине организована в следующих видах:
1. изучить теоретический материал по заданной теме;
2. выбрать методы решения поставленной задачи;
3. выполнить индивидуальные задания;
4. проанализировать полученные результаты;
5. отчитаться перед преподавателем по теоретической и практической части индивидуальной работы.