Негосударственное аккредитованное некоммерческое частное образовательное учреждение высшего образования
«Академия маркетинга и социально-информационных технологий – ИМСИТ»
(г. Краснодар)

(НАН ЧОУ ВО Академия ИМСИТ)

УТВЕРЖДАЮ
Проректор по учебной работе, доцент

_____Н.И. Севрюгина

20.11.2023

Б1.В.ДЭ.05.01
Экономика защиты информации
рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Кафедра бизнес-процессов и экономической безопасности**

Учебный план 10.03.01 Информационная безопасность

Квалификация **бакалавр**
Форма обучения **очная**
Общая трудоемкость **2 ЗЕТ**

Часов по учебному плану 72
в том числе:
аудиторные занятия 32
самостоятельная работа 39,8
контактная работа во время промежуточной аттестации (ИКР) 0

Виды контроля в семестрах:
зачеты 5

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**5 (3.1)**		Итого	
Недель	16 5/6			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Практические	16	16	16	16
Контактная работа на аттестации	0,2	0,2	0,2	0,2
Итого ауд.	32	32	32	32
Контактная работа	32,2	32,2	32,2	32,2
Сам. работа	39,8	39,8	39,8	39,8
Итого	72	72	72	72

Программу составил(и):

к.ю.н, доцент, Субачев С.Ю.

Рецензент(ы):

кандидат педагогических наук, доцент, доцент кафедры гуманитарных дисциплин Краснодарского филиала ФГБОУ ВО «Российский экономический университет имени Г.В. Плеханова», Кирий Е.В.;к.э.н., доцент, директор ООО «СофтСервис-Юг», г. Краснодар, Шупило О.М.

Рабочая программа дисциплины

Экономика защиты информации

разработана в соответствии с ФГОС ВО:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность (приказ Минобрнауки России от 17.11.2020 г. № 1427)

составлена на основании учебного плана:

10.03.01 Информационная безопасность

утвержденного учёным советом вуза от 20.11.2023 протокол № 3.

Рабочая программа одобрена на заседании кафедры

Кафедра бизнес-процессов и экономической безопасности

Протокол от 01.11.2023 г. № 4

Зав. кафедрой Маглинова Татьяна Григорьевна

Согласовано с представителями работодателей на заседании НМС, протокол № 3 от 20.11.2023.

Председатель НМС проф. Павелко Н.Н.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	формирование у обучающихся системы знаний по теоретическим основам и практическим аспектам
1.2	экономической безопасности государства, отдельных организаций и фирм, об основных экономических
1.3	проблемах за¬щиты информации, по экономическим основам формирования системы защиты информации,
1.4	обоснованию принимаемых решений в области информационной безопасности, по методам оценки
1.5	эффективности проектов построения систем защиты экономических объектов, а также подготовка к
1.6	профессиональной деятельности.
Задачи:	

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В.ДЭ.05
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Основы информационной безопасности
2.1.2	Методы и средства криптографической защиты информации
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Организация и управление службой защиты информации
2.2.2	Системы охраны и инженерной защиты информации
2.2.3	Производственная практика: Технологическая практика
2.2.4	Выполнение и защита выпускной квалификационной работы
2.2.5	Производственная практика: Преддипломная практика
2.2.6	Комплексная защита объектов информатизации

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ, ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ и планируемые результаты обучения	
ПК-9: Способен организовывать работы по обеспечению информационной безопасности в автоматизированных системах	
ПК-9.1: Формулирование правил работы персонала со средствами защиты информации	
Знать	
Уровень 1	Минимальный необходимый уровень знаний правил работы персонала со средствами защиты информации
Уровень 2	Уровень знаний правил работы персонала со средствами защиты информации в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний правил работы персонала со средствами защиты информации в объёме, соответствующем программе подготовки, без ошибок
ПК-9.2: Распределяет обязанности и полномочия персонала, обслуживающего защищённую автоматизированную систему	
Уметь	
Уровень 1	Продемонстрированы основные умения распределять обязанности и полномочия персонала, обслуживающего защищённую автоматизированную систему, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения распределять обязанности и полномочия персонала, обслуживающего защищённую автоматизированную систему, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения распределять обязанности и полномочия персонала, обслуживающего защищённую автоматизированную систему, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ПК-9.3: Сопоставляет результат работы персонала, обслуживающего защищённую автоматизированную систему, с целевыми показателями функционирования службы защиты информации	
Владеть	
Уровень 1	Имеется минимальный набор навыков сопоставления результатов работы персонала, обслуживающего защищённую автоматизированную систему, с целевыми показателями функционирования службы защиты информации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки сопоставления результатов работы персонала, обслуживающего защищённую автоматизированную систему, с целевыми показателями функционирования службы защиты информации с некоторыми недочётами
Уровень 3	Продемонстрированы навыки сопоставления результатов работы персонала, обслуживающего защищённую автоматизированную систему, с целевыми показателями функционирования службы защиты информации без ошибок и недочётов

ПК-10: Способен собирать, анализировать и систематизировать информацию по зафиксированным инцидентам информационной безопасности	
ПК-10.1: Соотносит инциденты информационной безопасности с характеристиками систем и средств защиты информации	
Знать	
Уровень 1	Минимальный необходимый уровень знаний соотношения инцидентов информационной безопасности с характеристиками систем и средств защиты информации
Уровень 2	Уровень знаний соотношения инцидентов информационной безопасности с характеристиками систем и средств защиты информации в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний соотношения инцидентов информационной безопасности с характеристиками систем и средств защиты информации в объёме, соответствующем программе подготовки, без ошибок
ПК-10.2: Обосновывает необходимость модернизации системы защиты информации автоматизированной системы	
Уметь	
Уровень 1	Продемонстрированы основные умения обосновывать необходимость модернизации системы защиты информации автоматизированной системы, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения обосновывать необходимость модернизации системы защиты информации автоматизированной системы, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения обосновывать необходимость модернизации системы защиты информации автоматизированной системы, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ПК-10.3: Формулирует правила применения мер защиты информации, направленные на устранение причин возникновения инцидентов информационной безопасности	
Владеть	
Уровень 1	Имеется минимальный набор навыков формулирования правил применения мер защиты информации, направленные на устранение причин возникновения инцидентов информационной безопасности с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки формулирования правил применения мер защиты информации, направленные на устранение причин возникновения инцидентов информационной безопасности с некоторыми недочётами
Уровень 3	Продемонстрированы навыки формулирования правил применения мер защиты информации, направленные на устранение причин возникновения инцидентов информационной безопасности без ошибок и недочётов
ПК-10.4: Формулирует правила протоколирования результатов мониторинга безопасности автоматизированных систем	
Знать	
Уровень 1	Минимальный необходимый уровень знаний Формулирует правила протоколирования результатов мониторинга безопасности автоматизированных систем
Уровень 2	Уровень знаний Формулирует правила протоколирования результатов мониторинга безопасности автоматизированных систем в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний Формулирует правила протоколирования результатов мониторинга безопасности автоматизированных систем в объёме, соответствующем программе подготовки, без ошибок
Уметь	
Уровень 1	Продемонстрированы основные умения Формулирует правила протоколирования результатов мониторинга безопасности автоматизированных систем, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения Формулирует правила протоколирования результатов мониторинга безопасности автоматизированных систем, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения Формулирует правила протоколирования результатов мониторинга безопасности автоматизированных систем, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
Владеть	
Уровень 1	Имеется минимальный набор навыков формулирования правил протоколирования результатов мониторинга безопасности автоматизированных систем с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки формулирования правил протоколирования результатов мониторинга безопасности автоматизированных систем с некоторыми недочётами
Уровень 3	Продемонстрированы навыки формулирования правил протоколирования результатов мониторинга безопасности автоматизированных систем без ошибок и недочётов

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)						
Код занятия	**Наименование разделов и тем /вид занятия/**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература и эл. ресурсы**	**Практ. подг.**
	Раздел 1. Раздел 1. Информация как важнейший ресурс экономики					
1.1	Введение в дисциплину «Экономика защиты информации» /Лек/	5	2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	
1.2	Экономические проблемы информационных ресурсов и защиты информации /Лек/	5	2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	
1.3	Экономическая безопасность /Лек/	5	2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	
1.4	Информация как товар, цена информации /Лек/	5	2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	
1.5	Определение экономической эффективности защиты информации - основные положения /Лек/	5	2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	
1.6	Введение в дисциплину «Экономика защиты информации» /Пр/	5	2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	
1.7	Экономические проблемы информационных ресурсов и защиты информации /Пр/	5	2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	
1.8	Экономическая безопасность /Пр/	5	2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	
1.9	Информация как товар, цена информации /Пр/	5	2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	

1.10	Определение экономической эффективности защиты информации - основные положения /Пр/	5	2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	
1.11	Законодательные акты, регулирующие экономические вопросы защиты информации. /Ср/	5	6,2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	
1.12	Экономические проблемы информационных ресурсов /Ср/	5	4,8	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	
1.13	Экономическая безопасность предприятия в рыночных условиях /Ср/	5	4,8	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	
1.14	Основные подходы к определению затрат на защиту информации /Ср/	5	4,8	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	
1.15	Проанализировать общий подход к оценке эффек-тивности защиты и страхования инфор¬мации. Изу-чить Закон РФ "Об информации, информатизации и защите информации" (№ 24-ФЗ от 20.02.95). /Ср/	5	4,8	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	
	Раздел 2. Раздел 2. Экономическая эффективность систем защиты информации					
2.1	Ущерб, наносимый информации /Лек/	5	2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	
2.2	Критерии эффективности систем защиты информации /Лек/	5	2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	
2.3	Оценка экономического эффекта защиты информации. Экономическая эффективность инвестиций в защиту информации /Лек/	5	2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	
2.4	Оценка экономического эффекта защиты информации. Экономическая эффективность инвестиций в защиту ин-формации /Пр/	5	2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	

2.5	Производственно-хозяйственная деятельность организаций как потребитель и источник экономической информации, подлежащей защите /Пр/	5	2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	
2.6	Страхование как метод защиты информаци /Пр/	5	2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	
2.7	Степени наносимого ущерба информации; методы и способы страхования информации; экономическая оценке ущерба от реализации угроз /Ср/	5	4,8	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	
2.8	Методы оценки эффективности систем защиты /Ср/	5	4,8	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	
2.9	Особенностях инвестиций в защиту информации /Ср/	5	4,8	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	
	Раздел 3. Промежуточная аттестация					
3.1	Зачет /КА/	5	0,2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

5.1. Контрольные вопросы и задания

1. Различие и взаимосвязь понятий абсолютной и относительной эффективности.
2. Предотвращение ущерба владельца информации как главная экономическая задача защиты информации.
3. Виды ущерба владельца информации, возникающего вследствие отсутствия защиты информации.
4. Факторы, влияющие на величину ущерба информации.
5. Необходимость обеспечения сопоставимости величин при экономических расчетах.
6. Методы обеспечения сопоставимости величин при расчетах эффективности защиты информации.
7. Принцип приведения расчетных величин по тождественности результатов.
8. Приведение расчетных величин по фактору времени.
9. Применение дисконтирования при расчетах разновременных затрат и результатов.
10. Принципиальные подходы к оценке экономического эффекта защиты информации.
11. Стоимостная оценка контрафактного использования информации на внутреннем рынке.
12. Понятие об основных и сопутствующих составляющих ущерба владельца информации.
13. Упущенная выгода как результат хищения, разрушения или модификации информации.
14. Стоимостная оценка контрафактного использования информации на внешнем рынке.
15. Стоимостная оценка ущерба владельца информации от нарушения его прав на интеллектуальную собственность.
16. Особенности определения ущерба от утраты прав на вознаграждение за использование промышленной собственности.
17. Значение и общая характеристика инвестиционной деятельности.

18. Роль инвестиций в защиту информации.
19. Источники инвестиций в защиту информации.
20. Факторы, учитываемые при оценке эффективности инвестиционных проектов в защиту информации.
21. Виды эффективности, подлежащие определению при оценке инвестиций в защиту информации.
22. Понятие о финансовой (коммерческой) эффективности инвестиций.
23. Бюджетная эффективность инвестиционных проектов.
24. Основные экономические показатели, характеризующие проекты инвестиций в защиту информации.
25. Понятие о чистом дисконтированном доходе.
26. Значение индекса доходности при оценке инвестиционного проекта по защите информации.
27. Внутренняя норма доходности как показатель уровня разработки проекта инвестиций.
28. Понятие о сроке окупаемости инвестиционного проекта.
29. Назначение и содержание экспертного метода определения эффективности инвестиций в защиту информации.
30. Сравнительная оценка расчетного и экспертного методов определения эффективности инвестиционных проектов по защите информации.
31. Условия, определяющие целесообразность применения балльного метода оценки проектов инвестиций, в защиту информации.
32. Понятие о коэффициенте фактической эффективности проектной организации.
33. Производственно-хозяйственная деятельность организации как источник экономической информации, подлежащей защите.
34. Товарная политика предприятия как потребитель и источник экономической информации, подлежащей защите.
35. Ценовая политика фирмы как потребитель и источник информации, подлежащей защите.
36. Сбытовая политика предприятия как источник экономической информации, подлежащей защите.
37. Значение бизнес-плана предприятия для привлечения инвестиций в защиту информации.
38. Маркетинг-план фирмы как источник и потребитель экономической информации, подлежащей защите
39. Производственный раздел бизнес-плана организации как источник экономической информации, подлежащей защите.
40. Понятие о рисках, виды рисков, их классификация.
41. Риски при защите информации.
42. Управление рисками.
43. Расчеты вероятности рисковых событий.
44. Понятие о математическом ожидании рисков при защите информации.
45. Роль страхования в производственно-хозяйственной деятельности.
46. Страхование как метод защиты информации.
47. Обязанности страхователя и страховщика при страховании информации.
48. Обстоятельства, влияющие на размер страховых выплат.
49. Критерии для выбора метода страхования при защите информации.
50. Цели и принципы функционально-стоимостного анализа.
51. Содержание и методы проведения функционально-стоимостного анализа.
52. Применение функционально-стоимостного анализа для выявления первоочередных объектов страхования при защите информации.

5.2. Темы письменных работ

1. Элементы информационных правоотношений
2. Классификация информационных ресурсов по признаку собственности, по доступу информации и ее использованию - схема
3. Государственная тайна – определение
4. Перечень сведений составляющих государственную тайну
5. Сведения, не подлежащие отнесению к государственной тайне и засекречиванию
6. Степени секретности сведений, составляющих государственную тайну
7. Коммерческая тайна – определение
8. Перечень информации, составляющей коммерческую тайну
9. Перечень мер по охране конфиденциальности информации
10. Перечень сведений, не подлежащих к отнесению к коммерческой тайне
11. Обязанности работодателя по охране конфиденциальности информации
12. Понятие персональной и профессиональной тайн
13. Понятие эффективности
14. Денежные затраты на автоматизацию – понятие
15. Капитальные затраты – понятие

16. Состав капитальных затрат
17. Состав эксплуатационных текущих расходов
18. Понятие эффективности информационных технологий
19. Основные показатели экономической эффективности
20. Экономический эффект - определение
21. Перечень основных источников экономии
22. Коэффициент экономической эффективности капитальных вложений – определение
23. Срок окупаемости капитальных вложений – понятие
24. Понятия расчетной и фактической эффективности
25. Понятие прямого и косвенного экономического эффекта
26. Способы определения экономической эффективности
27. Понятие базисного и отчетного периода

5.3. Фонд оценочных средств

Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это….
информационная война
информационное оружие
информационное превосходство

Информация не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения в преимущественное положение по сравнению с другими объектами.
служебная информация
коммерческая тайна
банковская тайна
конфиденциальная информация

Гарантия того, что конкретная информация доступна только тому кругу лиц, для которых она предназначена
конфиденциальность
целостность
доступность
аутентичность
аппелеруемость

Гарантия того, что АС ведет себя в нормальном и внештатном режиме так, как запланировано
надежность
точность
контролируемость
устойчивость
доступность

Способность системы к целенаправленному приспособлению при изменении структуры, технологических схем или условий функционирования, которое спасает владельца АС от необходимости принятия кардинальных мер по полной замене средств защиты на новые.
принцип системности
принцип комплексности
принцип непрерывной защиты
принцип разумной достаточности
принцип гибкости системы

В классификацию вирусов по способу заражения входят
опасные
файловые
резидентные
загрузочные
файлово -загрузочные
нерезидентные

Комплекс превентивных мер по защите конфиденциальных данных и информационных процессов на предприятии это…
комплексное обеспечение ИБ
безопасность АС
угроза ИБ
атака на АС
политика безопасности

Вирусы, не связывающие свои копии с файлами, а создающие свои копии на дисках, не изменяя других файлов, называются:
компаньон - вирусами

черви
паразитические
студенческие
призраки
стелс - вирусы
макровирусы

К видам системы обнаружения атак относятся :
системы, обнаружения атаки на ОС
системы, обнаружения атаки на конкретные приложения
системы, обнаружения атаки на удаленных БД
все варианты верны

Автоматизированная система должна обеспечивать
надежность
доступность
целостность
контролируемость

Основными компонентами парольной системы являются
интерфейс администратора
хранимая копия пароля
база данных учетных записей
все варианты верны

Некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации это ….
идентификатор пользователя
пароль пользователя
учетная запись пользователя
парольная система

К принципам информационной безопасности относятся
скрытость
масштабность
системность
законность
открытости алгоритмов

К вирусам изменяющим среду обитания относятся:
черви
студенческие
полиморфные
спутники

Охрана персональных данных, государственной служебной и других видов информации ограниченного доступа это…
Защита информации
Компьютерная безопасность
Защищенность информации
Безопасность данных

Система физической безопасности включает в себя следующие подсистемы:
оценка обстановки
скрытность
строительные препятствия
аварийная и пожарная сигнализация

Какие степени сложности устройства Вам известны
упрощенные
простые
сложные
оптические
встроенные

К механическим системам защиты относятся:
проволока
стена
сигнализация

вы

Какие компоненты входят в комплекс защиты охраняемых объектов:
сигнализация
охрана
датчики
телевизионная система

К выполняемой функции защиты относится:
внешняя защита
внутренняя защита
все варианты верны

Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных:
Защита информации
Компьютерная безопасность
Защищенность информации
Безопасность данных

Средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним это:
информационная война
информационное оружие
информационное превосходство

Информация позволяющая ее обладателю при существующих или возможных обстоятельствах увеличивать доходы, сохранить положение на рынке товаров, работ или услуг это:
государственная тайна
коммерческая тайна
банковская тайна
конфиденциальная информация

Гарантия того, что при хранении или передаче информации не было произведено несанкционированных изменений:
конфиденциальность
целостность
доступность
аутентичность
аппелеруемость

Гарантия точного и полного выполнения команд в АС:
надежность
точность
контролируемость
устойчивость
доступность

Уровень защиты, при котором затраты, риск, размер возможного ущерба были бы приемлемыми:
принцип системности
принцип комплексности
принцип непрерывности
принцип разумной достаточности
принцип гибкости системы

Совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты АС от заданного множества угроз безопасности:
Комплексное обеспечение информационной безопасности
Безопасность АС
Угроза информационной безопасности
атака на автоматизированную систему
политика безопасности

Особенностями информационного оружия являются:
системность
открытость
универсальность
скрытность

К функциям информационной безопасности относятся:

совершенствование законодательства РФ в сфере обеспечения информационной безопасности
выявление источников внутренних и внешних угроз

Страхование информационных ресурсов
защита государственных информационных ресурсов
подготовка специалистов по обеспечению информационной безопасности

К типам угроз безопасности парольных систем относятся
словарная атака
тотальный перебор
атака на основе психологии
разглашение параметров учетной записи
все варианты ответа верны

К вирусам не изменяющим среду обитания относятся:
черви
студенческие
полиморфные
спутники

Хранение паролей может осуществляться
в виде сверток
в открытом виде
в закрытом виде
в зашифрованном виде
все варианты ответа верны

Антивирусная программа принцип работы, которой основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых вирусов называется:
ревизором
иммунизатором
сканером
доктора и фаги

Выбрать недостатки имеющиеся у антивирусной программы ревизор:
неспособность поймать вирус в момент его появления в системе
небольшая скорость поиска вирусов
невозможность определить вирус в новых файлах (в электронной почте, на дискете)

В соответствии с особенностями алгоритма вирусы можно разделить на два класса:
вирусы изменяющие среду обитания, но не распространяющиеся
вирусы изменяющие среду обитания при распространении
вирусы не изменяющие среду обитания при распространении
вирусы не изменяющие среду обитания и не способные к распространению в дальнейшем

К достоинствам технических средств защиты относятся:
регулярный контроль
создание комплексных систем защиты
степень сложности устройства
Все варианты верны

К тщательно контролируемым зонам относятся:
рабочее место администратора
архив
рабочее место пользователя

К системам оповещения относятся:
инфракрасные датчики
электрические датчики
электромеханические датчики
электрохимические датчики

К оборонительным системам защиты относятся:
проволочные ограждения
звуковые установки
датчики
световые установки

Охранное освещение бывает:
дежурное
световое
тревожное

К национальным интересам РФ в информационной сфере относятся:
Реализация конституционных прав на доступ к информации
Защита информации, обеспечивающей личную безопасность
Защита независимости, суверенитета, государственной и территориальной целостности
Политическая экономическая и социальная стабильность
Сохранение и оздоровлении окружающей среды

Информационная безопасность это:
Состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз
Состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз
Состояние, когда не угрожает опасность информационным системам
Политика национальной безопасности России

Наиболее распространенные угрозы информационной безопасности:
угрозы целостности
угрозы защищенности
угрозы безопасности
угрозы доступности
угрозы конфиденциальности

Что относится к классу информационных ресурсов:
Документы
Персонал
Организационные единицы
Промышленные образцы, рецептуры и технологии
Научный инструментарий

Гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена:
конфиденциальность
доступность
аутентичность
целостность

Устройства осуществляющие воздействие на человека путем передачи информации через внечувственное восприятие:
Средства массовой информации
Психотропные препараты
Психотронные генераторы
Средства специального программно-технического воздействия

Злонамеренные действия в нематериальной сфере могут быть подразделены на два класса, какие?
Информационный саботаж
Физический саботаж
Информационные инфекции

Что не относится к информационной инфекции:
Троянский конь
Фальсификация данных
Черви
Вирусы
Логическая бомба

Деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения и несанкционированного доступа к защищаемой информации и от получения защищаемой информации:
защита информации от непреднамеренного воздействия
защита информации от несанкционированного воздействия
защита информации от несанкционированного доступа
*защита от утечки информации
Идентификатор субъекта доступа, который является его секретом:
*пароль
ключ
электронно-цифровая подпись
сертификат ключа подписи

Исследование возможности расшифрования информации без знания ключей:
криптология
криптоанализ
взлом
несанкционированный доступ

Состояние защищенности национальных интересов страны в информационной сфере от внутренних и внешних угроз это:
Информационная безопасность
Безопасность
Национальная безопасность
Защита информации
Охрана персональных данных, государственной, служебной и других видов информации ограниченного доступа это:
Защита информации
Компьютерная безопасность
Защищенность информации
Защищенность потребителей информации
Безопасность данных

Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это:
Информационная война
Информационное оружие
Информационное превосходство

Реализация конституционных прав и свобод человека, обеспечение личной безопасности, повышение качества и уровня жизни это:
Интересы государства
Интересы государства в информационной сфере
Интересы личности
Интересы личности в информационной сфере
Интересы общества в информационной сфере

Информация, не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения, в преимущественное положение по сравнению с другими объектами:
Служебная информация
Коммерческая тайна
Банковская тайна
Конфиденциальная информация
Действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы.
Комплексное обеспечение информационной безопасности
Безопасность АС
Угроза информационной безопасности
Атака на автоматизированную систему
Политика безопасности

Вся накопленная информация об окружающей нас дейст вительности, зафиксированная на материальных носителях или в любой другой форме, обеспечивающая ее передачу во времени и пространстве между различными потребителями для решения научных, производст венных, управленческих и других задач
Информационные ресурсы
Информационная система
Информационная сфера
Информационные услуги
Информационные продукты

К какому уровню доступа информации относится следующая информация: «Информация, содержащая сведения об обстоятельствах и фактах, предоставляющих угрозу жизни, здоровью граждан …»
Информация без ограничения права доступа
Информация с ограниченным доступом
Информация, распространение которой наносит вред интересам общества
Объект интеллектуальной собственности
Иная общедоступная информация

Состояние защищенности при котором не угрожает опасность это:
Информационная безопасность
*Безопасность
Защита информации

Национальная безопасность

Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных:
Защита информации
Компьютерная безопасность
Защищенность информации
Защищенность потребителей информации

Особый вид отношений между государствами, при котором для разрешения существующих межгосударственных противоречий используются методы, средства и технологии силового воздействия на информационную сферу этих государств:
Информационная война
Информационное оружие
Информационное превосходство

Создание условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя , суверенитета и территориальной целостности это:
Интересы государства
Интересы государства в информационной сфере
Интересы личности
Интересы личности в информационной сфере
Интересы общества в информационной сфере

Информационно упорядоченная совокупность документов и информационных технологий, реализующая информационные процессы
Информационные ресурсы
Информационная система
Информационная сфера
Информационные услуги
Информационные продукты

К какому уровню доступа информации относится следующая информация: «Авторское право, патентное право…»
Информация без ограничения права доступа
Информация с ограниченным доступом
Информация, распространение которой наносит вред интересам общества
Объект интеллектуальной собственности
Иная общедоступная информация

Состояние защищенности многонационального народа как носителя суверенитета и единственного источника власти:
Информационная безопасность
Безопасность
Защита информации
Национальная безопасность

Защита от случайных и преднамеренных воздействий, чреватых нанесением ущерба владельцам или пользователям информации это:
Защита информации
Компьютерная безопасность
Защищенность информации
Защищенность потребителей информации

Средства уничтожения, искажения, или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним это:
Информационная война
Информационное оружие
Информационное превосходство

Документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ:
Государственная тайна
Коммерческая тайна
Банковская тайна
Конфиденциальная информация

Свойство данных быть доступными для санкционированного пользования в произвольный момент времени, когда в обращении к ним возникает необходимость:
Конфиденциальность
Целостность

Доступность
Аутентичность
Аппелируемость

Гарантия того, что в любой момент времени может быть произведена полноценная проверка любого компонента программного комплекса АС:
Надежность
Точность
Контролируемость
Устойчивость
Доступность

Непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС:
Принцип системности
Принцип комплексности
Принцип непрерывной защиты
Принцип разумной достаточности
Принцип гибкости системы

Возможные воздействия на АС, которые прямо или косвенно могут нанести ущерб ее безопасности:
Комплексное обеспечение информационной безопасности
Безопасность АС
Угрозы информационной безопасности
Атака на автоматизированную систему
Политика безопасности
Совокупность информации, информационной структуры субъектов, осуществляющих сбор, формирование, распространение и использование информации, а так же системы регулирования возникающих при этом общественных отношений
Информационные ресурсы
Информационная система
Информационная сфера
Информационные услуги
Информационные продукты

К какому уровню доступа информации относится следующая информация: «Ложная реклама, реклама со скрытыми вставками…»
Информация без ограничения права доступа
Информация с ограниченным доступом
Информация, распространение которой наносит вред интересам общества
Объект интеллектуальной собственности
Иная общедоступная информация
Защищенность страны от нападения извне, шпионажа, покушения на государственный и общественный строй:
Информационная безопасность
Безопасность
Национальная безопасность
Защита информации
Защищенность от негативных информационно-психологических и информационно- технических воздействий:
Защита информации
Компьютерная безопасность
Защищенность информации
Защищенность потребителей информации

Возможность сбора, обработки и распространения непрерывного потока информации при воспрещении использования информации противником это:
Информационная война
Информационное оружие
Информационное превосходство
Обобщение интересов личности в этой сфере, упрочнение демократии, создание правового государства это:
Интересы государства
Интересы государства в информационной сфере
Интересы личности в информационной сфере
Интересы общества
Интересы общества в информационной сфере
Защищаемые государством сведения в области военной, внешнеполитической и внешнеэкономической деятельности, распространение которых может нанести ущерб безопасности РФ.
Государственная тайна
Коммерческая тайна

Банковская тайна
Конфиденциальная информация

Гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор:
Конфиденциальность
Целостность
Доступность
Аутентичность
Аппелируемость

Гарантия того, что при умышленном внесении ошибок в пределах заранее оговоренных норм АС будет вести себя так, как оговорено заранее:
Надежность
Точность
Контролируемость
Устойчивость
Доступность

Согласование разнородных средств при построении целостной системы защиты, перекрывающий все существенные каналы реализации угроз и не содержащий слабых мест на стыках отдельных компонентов:
Принцип системности
Принцип комплексности
Принцип непрерывной защиты
Принцип разумной достаточности
Принцип гибкости системы

Защищенность АС от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, изменения или разрушения ее компонентов:
Комплексное обеспечение информационной безопасности
Безопасность АС
Угроза информационной безопасности
Атака на автоматизированную систему
Политика безопасности
Действие субъектов по обеспечению пользователей информационными продуктами:
Информационные ресурсы
Информационная система
Информационная сфера
Информационные услуги
Информационные продукты

К какому уровню доступа информации относится следующая информация: «Библиографические и опознавательные данные, личные характеристики , сведения о семейном положении, сведения об имущественном или финансовом состоянии…»
Информация без ограничения права доступа
Информация с ограниченным доступом
Информация, распространение которой наносит вред интересам общества
Объект интеллектуальной собственности
Иная общедоступная информация

Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов и требований:
Защищенность информации
Защищаемая информация
Защищенность потребителей информации
Защита информации

Действия предпринимаемые для достижения информационного превосходства в поддержке национальной информационной стратегии посредством воздействия на информацию и информационные системы противника:
Информационная война
Информационное оружие
Информационное превосходство
Гарантия неразглашения банковского счета, операций по счету и сведений о клиенте:
Государственная тайна
Коммерческая тайна
Банковская тайна
Конфиденциальная информация

Гарантия того, что при необходимости можно будет доказать, что автором сообщения является именно тот человек,

который заявлен как ее автор и ни кто другой:
Конфиденциальность
Целостность
Доступность
Аутентичность
Аппелируемость

Системный подход к защите компьютерных систем предполагающий необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов:
Принцип системности
Принцип комплексности
Принцип непрерывной защиты
Принцип разумной достаточности
Принцип гибкости системы

Область науки и техники, охватывающая совокупность криптографических, программно-аппаратных, технических, правовых, организационных методов и средств обеспечения безопасности информации при ее обработке, хранении и передаче с использованием современных информационных технологий:
Комплексное обеспечение информационной безопасности
Безопасность АС
Угроза безопасности
Атака на автоматизированную систему
Политика безопасности

Документированная информация, подготовленная в соответствии с потребностями пользователей и предназначенная или применяемая для удовлетворения потребностей пользователей:
Информационные ресурсы
Информационная система
Информационная сфера
Информационные услуги
Информационные продукты

К какому уровню доступа информации относится следующая информация: «Информация в области работ по хранению, перевозке, уничтожению химического оружия – сведения о состоянии здоровья граждан и объектов окружающей среды в районах размещения объектов по уничтожению химического оружия…»
Информация без ограничения права доступа
Информация с ограниченным доступом
Информация, распространение которой наносит вред интересам общества
Объект интеллектуальной собственности
Иная общедоступная информация

Соотнесите интересы в области информационной безопасности:
Национальные интересы
Интересы личности
Интересы государства
Интересы общества

1. Информация как фактор производства.
2. Значение экономической информации для развития рынка.
3. Информация о рынке как основа долгосрочного прогнозирования экономического развития.
4. Информация как ресурс экономики.
5. Основные характеристики продукта как товара.
6. Стоимость товара, методы ее определения.
7. Особенности информации как товара.
8. Составляющие себестоимости информационных массивов.
9. Особенности стоимостной оценки интеллектуального труда.
10. Формирование цены на информацию в рыночных условиях.
11. Понятие об экономической безопасности.
12. Факторы экономической безопасности государства.
13. Экономическая безопасность фирмы, предприятия.
14. Экономическая безопасность личности.
15. Правовые основы обеспечения экономической безопасности.
16. Методы обеспечения экономической безопасности фирмы, предприятия.
17. Взаимосвязь экономической и информационной безопасности.
18. Понятия об экономическом эффекте и экономической эффективности.

5.4. Перечень видов оценочных средств
Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа на теоретический вопрос. Задание с выбором варианта ответа (ОВ, в задании данного типа предлагается несколько вариантов ответа, среди которых верный(ые). Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа, включающего полное решение задачи с пояснениями.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Дергачев К. В., Титарев Д. В.	Защита информации: лабораторный практикум: Учебное пособие	Москва: Русайнс, 2021, URL: https://book.ru/book/940250
Л1.2	Москвитин Г. И.	Комплексная защита информации в организации: Монография	Москва: Русайнс, 2020, URL: https://book.ru/book/934814
Л1.3	Жук А.П., Жук Е.П.	Защита информации: Учебное пособие	Москва: Издательский Центр РИО□, 2021, URL: http://znanium.com/catalog/document?id=367588

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Сычев Ю.Н.	Защита информации и информационная безопасность: Учебное пособие	Москва: ООО "Научно-издательский центр ИНФРА-М", 2021, URL: http://znanium.com/catalog/document?id=366835
Л2.2	Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РИО□, 2022, URL: https://znanium.com/catalog/document?id=393765

6.3.1. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

6.3.1.1	Windows 10 Pro RUS Операцинная система – Windows 10 Pro RUS Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2021
6.3.1.2	7-Zip Архиватор 7-Zip Программное обеспечение по лицензии GNU GPL
6.3.1.3	Яндекс Браузер Браузер Яндекс Браузер Лицензионное соглашение на использование программ Яндекс Браузер https://yandex.ru/legal/browser_agreement/
6.3.1.4	LibreOffice Офисный пакет LibreOffice Программное обеспечение по лицензии GNU GPL

6.3.2. Перечень профессиональных баз данных и информационных справочных систем

6.3.2.1	Консультант Плюс http://www.consultant.ru
6.3.2.2	Кодекс – Профессиональные справочные системы https://kodeks.ru

7. МТО (оборудование и технические средства обучения)

Ауд	Наименование	ПО	Оснащение
230	Кабинет гуманитарных и социально-экономических дисциплин	7-Zip Яндекс Браузер Mozilla Firefox LibreOffice	Парта ученическая со скамьей (2-местная) – 14 шт., рабочее место преподавателя– 1 шт., доска учебная - 1 шт., персональный компьютер - 1 шт., многофункциональное устройство – 1 шт., мультимедийный проектор – 1 шт., учебно-методическая литература, учебно-наглядные методические пособия, соответствующее программное обеспечение
121	Компьютерный класс	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. 1С:Предприятие 8. Комплект Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS SQL Server 2019	Стол - 20 шт., стул - 21 шт., рабочее место преподавателя – 1 шт., персональный компьютер с выходом в интернет - 21 шт., доска учебная – 1 шт., многофункциональное устройство – 1 шт., мультимедийный проектор – 1 шт., проекционный экран – 1 шт., соответствующее программное обеспечение

		MS SQL Server Management Studio 18.8 MS Visio Pro 2016 MS Visual Studio Community Edition Visual Studio Code Blender Gimp Maxima Oracle VM VirtualBox StarUML V1 PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclips Adobe Reader DC Arduino Software (IDE) NetBeans IDE ZEAL ARIS Express Archimate ПО ЛИНКО v8.2 демо-версия Klite Mega Codec Pack Ramus Educational Micro-Cap Evaluation gvSIG Desktop Python	
Читальный зал	Информационно-библиотечный центр (помещение для самостоятельной работы обучающихся)	7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS Visio Pro 2016 Visual Studio Code Blender Gimp Maxima IntelliJ IDEA PyCharm Community Edition Adobe Reader DC MS Office Standart 2007 Windows 10 Pro	Стол - 20 шт., стул - 20 шт., рабочее место сотрудника - 2 шт., персональный компьютер с выходом в интернет и обеспечением доступа в электронную информационно-образовательную среду академии – 17 шт., многофункциональное устройство – 2 шт.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

В соответствии с требованиями ФГОС ВО по направлению подготовки реализация компетентностного подхода предусматривает использование в учебном процессе активных и интерактивных форм проведения занятий (разбор конкретных задач, проведение блиц-опросов, исследовательские работы) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Лекционные занятия дополняются ПЗ и различными формами СРС с учебной и научной литературой В процессе такой работы студенты приобретают навыки «глубокого чтения» - анализа и интерпретации текстов по методологии и методике дисциплины.

Учебный материал по дисциплине «Экономика защиты информации», разделен на логически завершенные части (модули), после изучения, которых предусматривается аттестация в форме письменных тестов, контрольных работ.

Работы оцениваются в баллах, сумма которых дает рейтинг каждого обучающегося. В баллах оцениваются не только знания и навыки обучающихся, но и их творческие возможности: активность, неординарность решений поставленных проблем. Каждый модуль учебной дисциплины включает обязательные виды работ – лекции, ПЗ, различные виды СРС (выполнение домашних заданий по решению задач, подготовка к лекциям и практическим занятиям).

Форма текущего контроля знаний – работа студента на практическом занятии, опрос. Форма промежуточных аттестаций – контрольная работа в аудитории, домашняя работа. Итоговая форма контроля знаний по модулям – контрольная работа с задачами по материалу модуля.

Методические указания по выполнению всех видов учебной работы размещены в электронной образовательной среде академии.

Методические указания и материалы по видам учебных занятий по дисциплине:
Вид учебных занятий, работ - Организация деятельности обучающегося
Лекция - Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения, отмечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, попытаться найти ответ в рекомендуемой литературе, если самостоятельно не удаётся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.
Практические занятия - Конспектирование источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, работа с текстом. Выполнение практических задач в инструментальных средах. Выполнение проектов. Решение расчётно-графических заданий, решение задач по алгоритму и др.
Самостоятельная работа - Знакомство с основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующихся для запоминания и являющихся основополагающими в этой теме. Составление аннотаций к прочитанным литературным источникам и др.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ОБУЧАЮЩИМСЯ ПО ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Методические указания по выполнению самостоятельной работы по дисциплине «Экономика защиты информации».
Формой осуществления контроля выполнения самостоятельной работы является подготовки рефератов на актуальные темы,
т. е. изучение с помощью научных методов явлений и процессов, анализа влияния на них различных факторов, а также, изучение взаимодействия между явлениями, с целью получения убедительно доказанных и полезных для науки и практики решений с максимальным эффектом.
Цель реферата – определение конкретного объекта и всестороннее, достоверное изучение его структуры, характеристик, связей на основе разработанных в науке принципов и методов познания, а также получение полезных для деятельности человека результатов, внедрение в производство с дальнейшим эффектом.
Основой разработки каждой темы является методология, т. е. совокупность методов, способов, приемов и их определенная последовательность, принятая при разработке научного исследования. В конечном счете, методология – это схема, план решения поставленной научно исследовательской задачи.
Процесс подготовки реферата состоит из следующих основных этапов:
1. Выбор темы и обоснование ее актуальности.
2. Составление библиографии, ознакомление с законодательными актами, нормативными документами и другими источниками, относящимися к теме проекта (работы).
3. Разработка алгоритма исследования, формирование требований к исходным данным, выбор методов и инструментальных
средств анализа.
4. Сбор фактического материала.
5. Обработка и анализ полученной информации с применением современных методов анализа.
6. Формулировка выводов и выработка рекомендаций.
7. Оформление работы в соответствии с установленными требованиями