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.О.40
Основы управления информационной безопасностью
рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Кафедра государственного и корпоративного управления**

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 7

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	15 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
В том числе в форме практ.подготовки	4	4	4	4
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):

преподаватель, Большакова М.В.

Рецензент(ы):

Первый заместитель начальника управления инвестиций и развития малого и среднего предпринимательства администрации муниципального образования город Краснодар, начальник отдела муниципально-частного партнерства, Алешин Антон Сергеевич;кэн, Заместитель начальника отдела по финансовому и фондовому рынку и жилищным программам управления экономики администрации муниципального образования город Краснодар ., Макаренко Юлия Григорьевна

Рабочая программа дисциплины

Основы управления информационной безопасностью

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 государственного и корпоративного управления

Протокол от 01.11.2023 г. № 4

Зав. кафедрой Мугаева Екатерина Викторовна

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	Целью освоения учебной дисциплины является изучение методов и средств
1.2	управления информационной безопасностью (ИБ) в организации, а также изучение основных
1.3	подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию
1.4	систем управления информационной безопасностью (СУИБ) определенного объекта.
Задачи: привитие обучаемым основ культуры обеспечения информационной безопасности; формирование у обучаемых понимания роли процессов управления в обеспечении информационной безопасности организаций, объектов и систем; ознакомление обучаемых с основными методами управления информационной безопасностью организаций, объектов и систем; обучение различным методам реализации процессов управления информационной безопасностью, направленных на эффективное управление ИБ конкретной организации.	

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Интеллектуальные системы и технологии
2.1.2	Организационное и правовое обеспечение информационной безопасности
2.1.3	Учебная практика: Учебно-лабораторная практика
2.1.4	Структуры и алгоритмы обработки данных
2.1.5	Защита информации от утечки по техническим каналам
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Выполнение и защита выпускной квалификационной работы
2.2.2	Производственная практика: Преддипломная практика
2.2.3	Производственная практика: Эксплуатационная практика

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ, ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ и планируемые результаты обучения	
ОПК-1: Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;	
ОПК-1.1: Классифицирует угрозы информационной безопасности в соответствии с нормативными документами	
Знать	
Уровень 1	Минимальный необходимый уровень знаний классификации угроз информационной безопасности в соответствии с нормативными документами
Уровень 2	Уровень знаний классификации угроз информационной безопасности в соответствии с нормативными документами в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний классификации угроз информационной безопасности в соответствии с нормативными документами в объёме, соответствующем программе подготовки, без ошибок
ОПК-1.2: Оценивает угрозы информационной безопасности с точки зрения основных концепций национальной безопасности Российской Федерации	
Уметь	
Уровень 1	Продемонстрированы основные умения оценки угроз информационной безопасности с точки зрения основных концепций национальной безопасности Российской Федерации , решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения оценки угроз информационной безопасности с точки зрения основных концепций национальной безопасности Российской Федерации, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения оценки угроз информационной безопасности с точки зрения основных концепций национальной безопасности Российской Федерации, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ОПК-1.3: Определяет угрозы информационной безопасности для различных систем	
Владеть	
Уровень 1	Имеется минимальный набор навыков определения угроз информационной безопасности для различных систем с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки определения угроз информационной безопасности для различных систем с некоторыми недочётами
Уровень 3	Продемонстрированы навыки определения угроз информационной безопасности для различных систем без ошибок и недочётов

ОПК-5: Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;	
ОПК-5.1: Разрабатывает проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации	
Знать	
Уровень 1	Минимальный необходимый уровень знаний особенностей разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации
Уровень 2	Уровень знаний особенностей разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний особенностей разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации в объёме, соответствующем программе подготовки, без ошибок
ОПК-5.2: Формулирует основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации	
Уметь	
Уровень 1	Продемонстрированы основные умения формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ОПК-5.3: Формулирует основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации	
Владеть	
Уровень 1	Имеется минимальный набор навыков формулирования основных требований при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки формулирования основных требований при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации с некоторыми недочётами
Уровень 3	Продемонстрированы навыки формулирования основных требований при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации без ошибок и недочётов

ОПК-6: Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	
ОПК-6.1: Разрабатывает модели угроз и модели нарушителя объекта информатизации	
Знать	
Уровень 1	Минимальный необходимый уровень знаний моделей угроз и модели нарушителя объекта информатизации
Уровень 2	Уровень знаний моделей угроз и модели нарушителя объекта информатизации в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний моделей угроз и модели нарушителя объекта информатизации в объёме, соответствующем программе подготовки, без ошибок
ОПК-6.2: Определяет политику контроля доступа работников к информации ограниченного доступа	
Уметь	
Уровень 1	Продемонстрированы основные умения определения политики контроля доступа работников к информации ограниченного доступа, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения определения политики контроля доступа работников к информации ограниченного доступа, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами

Уровень 3	Продемонстрированы все основные умения определения политики контроля доступа работников к информации ограниченного доступа, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ОПК-6.3: Формулирует требования, предъявляемые к физической защите объекта и пропускному режиму в организации	
Владеть	
Уровень 1	Имеется минимальный набор навыков формулирования требований, предъявляемых к физической защите объекта и пропускному режиму в организации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки формулирования требований, предъявляемых к физической защите объекта и пропускному режиму в организации с некоторыми недочётами
Уровень 3	Продемонстрированы навыки формулирования требований, предъявляемых к физической защите объекта и пропускному режиму в организации без ошибок и недочётов
ОПК-6.4: Разрабатывает проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации	
Знать	
Уровень 1	Минимальный необходимый уровень знаний Разрабатывает модели угроз и модели нарушителя объекта информатизации
Уровень 2	Уровень знаний Разрабатывает модели угроз и модели нарушителя объекта информатизации в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний Разрабатывает модели угроз и модели нарушителя объекта информатизации в объёме, соответствующем программе подготовки, без ошибок
Уметь	
Уровень 1	Продемонстрированы основные умения Определяет политику контроля доступа работников к информации ограниченного доступа, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения Определяет политику контроля доступа работников к информации ограниченного доступа, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения Определяет политику контроля доступа работников к информации ограниченного доступа, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
Владеть	
Уровень 1	Имеется минимальный набор навыков разработки проектов инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки разработки проектов инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации с некоторыми недочётами
Уровень 3	Продемонстрированы навыки разработки проектов инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации без ошибок и недочётов

ОПК-12: Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	
ОПК-12.1: Определяет информационную инфраструктуру и информационные ресурсы организации, подлежащие защите	
Знать	
Уровень 1	Минимальный необходимый уровень знаний определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите
Уровень 2	Уровень знаний определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите в объёме, соответствующем программе подготовки, без ошибок
ОПК-12.2: Анализирует показатели качества и критерии оценки систем и отдельных методов и средств защиты информации	
Уметь	
Уровень 1	Продемонстрированы основные умения анализирования показателей качества и критериев оценки систем и отдельных методов и средств защиты информации, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения Анализирует показатели качества и критерии оценки систем и отдельных методов и средств защиты информации, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения Анализирует показатели качества и критерии оценки систем и

	отдельных методов и средств защиты информации, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ОПК-12.3: Оценивает информационные риски в автоматизированных системах	
Владеть	
Уровень 1	Имеется минимальный набор навыков оценки информационных рисков в автоматизированных системах области с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки оценки информационных рисков в автоматизированных системах области с некоторыми недочётами
Уровень 3	Продемонстрированы навыки оценки информационных рисков в автоматизированных системах области без ошибок и недочётов
ОПК-12.4: Разрабатывает основные показатели технико-экономического обоснования соответствующих проектных решений	
Знать	
Уровень 1	Минимальный необходимый уровень знаний Определяет информационную инфраструктуру и информационные ресурсы организации, подлежащие защите
Уровень 2	Уровень знаний Определяет информационную инфраструктуру и информационные ресурсы организации, подлежащие защите в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний Определяет информационную инфраструктуру и информационные ресурсы организации, подлежащие защите в объёме, соответствующем программе подготовки, без ошибок
Уметь	
Уровень 1	Продемонстрированы основные умения Анализирует показатели качества и критерии оценки систем и отдельных методов и средств защиты информации, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения Анализирует показатели качества и критерии оценки систем и отдельных методов и средств защиты информации, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения Анализирует показатели качества и критерии оценки систем и отдельных методов и средств защиты информации, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
Владеть	
Уровень 1	Имеется минимальный набор навыков разработки основных показателей технико-экономического обоснования соответствующих проектных решений с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки разработки основных показателей технико-экономического обоснования соответствующих проектных решений с некоторыми недочётами
Уровень 3	Продемонстрированы навыки разработки основных показателей технико-экономического обоснования соответствующих проектных решений без ошибок и недочётов

ОПК-4.1: Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах;	
ОПК-4.1.1: Определяет подлежащие защите информационные ресурсы автоматизированных систем	
Уметь	
Уровень 1	Продемонстрированы основные умения определения подлежащих защите информационных ресурсов автоматизированных систем, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения определения подлежащих защите информационных ресурсов 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 определения подлежащих защите информационных ресурсов автоматизированных систем, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ОПК-4.1.2: Составляет комплексы правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	
Уметь	
Уровень 1	Продемонстрированы основные умения составления комплексов правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения составления комплексов правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные составления комплексов правил, процедур, практических приемов,

	принципов и методов, средств обеспечения защиты информации в автоматизированной системе, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ОПК-4.1.3: Организует работу персонала автоматизированной системы с учетом требований по защите информации	
Владеть	
Уровень 1	Имеется минимальный набор навыков организации работы персонала автоматизированной системы с учетом требований по защите информации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки организации работы персонала автоматизированной системы с учетом требований по защите информации с некоторыми недочётами
Уровень 3	Продемонстрированы базовые навыки Организует работу персонала автоматизированной системы с учетом требований по защите информации без ошибок и недочётов
ОПК-4.1.4: Готовит документы, определяющие правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации	
Владеть	
Уровень 1	Имеется минимальный набор навыков подготовки документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки подготовки документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации с некоторыми недочётами
Уровень 3	Продемонстрированы базовые навыки подготовки документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации 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. Учебный модуль 1. Основы и системы управления информационной безопасностью (ИБ)					
1.1	Введение. Важность и актуальность дисциплины. Ее взаимосвязь с другими дисциплинами специальности. Содержание дисциплины. Виды контроля знаний. /Лек/	7	4	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-5.1 ОПК-5.2 ОПК-5.3 ОПК-6.1 ОПК-6.2 ОПК-6.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7	

1.2	Базовые вопросы управления ИБ. Сущность и функции управления. Наука управления. Принципы, подходы и виды управления. Цели и задачи управления ИБ. Понятие системы управления. /Пр/	7	4	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-5.1 ОПК-5.2 ОПК-5.3 ОПК-6.1 ОПК-6.2 ОПК-6.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7	2
1.3	Стандартизация в области управления ИБ. Стандартизация в области построения систем управления. История развития. Существующие стандарты и методологии по управлению ИБ: их отличия, сильные и слабые стороны (на примере семейства стандартов ISO/IEC 2700x, СТО БР ИББС-1.0, ГОСТ Р ИСО/МЭК 17799, ГОСТ Р ИСО/МЭК 27001, ISO/IEC 18044, BS 25999 и др.). /Ср/	7	6,8	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-5.1 ОПК-5.2 ОПК-5.3 ОПК-6.1 ОПК-6.2 ОПК-6.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.4	Процессный подход. Понятие процесса. Методы формализации процессов. Цели и задачи формализации процессов. Понятие процессного подхода. Процессный подход к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления (на примере СУИБ). Понятие СУИБ. Место СУИБ в рамках общей системы управления предприятием. Основные процессы СУИБ и требования, предъявляемые к ним каждым из стандартов. /Лек/	7	4	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-5.1 ОПК-5.2 ОПК-5.3 ОПК-6.1 ОПК-6.2 ОПК-6.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7	

1.5	Область деятельности СУИБ. Понятие области деятельности СУИБ. Механизм выбора области деятельности. Состав области деятельности (процессы, структурные подразделения организации, кадры). Описание области деятельности (структура и содержание документа). /Пр/	7	4	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-5.1 ОПК-5.2 ОПК-5.3 ОПК-6.1 ОПК-6.2 ОПК-6.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7	2
1.6	Ролевая структура СУИБ. Понятие роли. Использование ролевого принципа в рамках СУИБ. Преимущества использования ролевого принципа. Ролевая структура СУИБ (основные и дополнительные роли). Роль высшего руководства организации в СУИБ. Этапы разработки и функционирования СУИБ, на которых важно участие руководства организации. Суть участия руководства организации на этих этапах (утверждение документов, результатов анализа рисков и т.д.) /Ср/	7	6,8	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-5.1 ОПК-5.2 ОПК-5.3 ОПК-6.1 ОПК-6.2 ОПК-6.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
	Раздел 2. Учебный модуль 2. Основы управления рисками, процессы управления ИБ					
2.1	Рискология ИБ. Основные определения и положения рискологии. Цель процесса анализа рисков ИБ. Этапы и участники процесса анализа рисков ИБ. /Лек/	7	4	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-5.1 ОПК-5.2 ОПК-5.3 ОПК-6.1 ОПК-6.2 ОПК-6.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7	

2.2	Анализ рисков ИБ. Методики анализа рисков ИБ. Инвентаризация активов. Понятие актива. Типы активов. Источники информации об активах организации. Определение угроз ИБ и уязвимостей для выделенных на этапе инвентаризации активов. Оценка рисков ИБ. Планирование мер по обработке выявленных рисков ИБ. Утверждение результатов анализа рисков ИБ у высшего руководства. Использование результатов анализа рисков ИБ. /Пр/	7	4	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-5.1 ОПК-5.2 ОПК-5.3 ОПК-6.1 ОПК-6.2 ОПК-6.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
2.3	Основные процессы СУИБ. Обязательная документация СУИБ. Процессы «Управление документами» и «Управление записями» (цели и задачи процессов, входные/выходные данные, роли участников, обязательные этапы процессов, связи с другими процессами СУИБ). Процессы улучшения СУИБ («Внутренний аудит», «Корректирующие действия», «Предупреждающие действия»). Процесс «Мониторинг эффективности» (включая разработку метрик эффективности). Понятие «Зрелость процесса». «Анализ со стороны высшего руководства». Процесс «Обучение и обеспечение осведомленности». /Ср/	7	6,8	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-5.1 ОПК-5.2 ОПК-5.3 ОПК-6.1 ОПК-6.2 ОПК-6.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
2.4	Внедрение разработанных процессов. Документ «Положение о применимости». Этапы внедрения процессов и их последовательность. Обучение сотрудников, как один из этапов внедрения. Сложности, возникающие при внедрении процессов управления ИБ, и способы их решения. Контроль над внедрением процессов. Документирование процесса внедрения разработанных процессов. Типовой документ «Положение о применимости». Цель документа. Структура и содержание документа. Процесс разработки документа, решение спорных ситуаций при разработке документа. /Лек/	7	4	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-5.1 ОПК-5.2 ОПК-5.3 ОПК-6.1 ОПК-6.2 ОПК-6.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7	

2.5	. Внедрение мер (контрольных процедур) по обеспечению ИБ. Категории контрольных процедур. Перечень контрольных процедур по обеспечению ИБ в соответствии с лучшими международными практиками. Содержание контрольных процедур по обеспечению ИБ в интерпретации лучших практик. /Пр/	7	4	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-5.1 ОПК-5.2 ОПК-5.3 ОПК-6.1 ОПК-6.2 ОПК-6.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
2.6	Процесс «Управление инцидентами ИБ». Цели и задачи процесса «Управления инцидентами ИБ, важность процесса с точки зрения управления ИБ. Входные/выходные данные процесса. Участники процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ. /Ср/	7	6,8	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-5.1 ОПК-5.2 ОПК-5.3 ОПК-6.1 ОПК-6.2 ОПК-6.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
2.7	Процесс «Обеспечение непрерывности ведения бизнеса». Цели и задачи процесса «Обеспечение непрерывности ведения бизнеса». Входные/выходные данные процесса. Участники процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ. /Ср/	7	6,8	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-5.1 ОПК-5.2 ОПК-5.3 ОПК-6.1 ОПК-6.2 ОПК-6.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7	

2.8	Эксплуатация и независимый аудит СУИБ. Ввод системы в эксплуатацию. Возможные проблемы и способы их решения. Внешние аудиты ИБ на соответствие требованиям нормативных документов. Этапы проведения аудита ИБ. Результаты аудита ИБ и их интерпретация. Сертификация по ISO/IEC 27001 или ГОСТ Р ИСО/МЭК 27001. /Ср/	7	5,8	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-5.1 ОПК-5.2 ОПК-5.3 ОПК-6.1 ОПК-6.2 ОПК-6.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
	Раздел 3. Промежуточная аттестация					
3.1	Зачет /КА/	7	0,2	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-5.1 ОПК-5.2 ОПК-5.3 ОПК-6.1 ОПК-6.2 ОПК-6.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7	

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

5.1. Контрольные вопросы и задания

1. Основные понятия информационной безопасности.
2. Угрозы информационной безопасности в информационных системах.
3. Оценочные стандарты в информационной безопасности.
4. Стандарты управления информационной безопасностью.
5. Создание СУИБ на предприятии.
6. Методика оценки рисков информационной безопасности компании Digital Security.
7. Методики и технологии управления рисками.
8. Разработка корпоративной методики анализа рисков.
9. Современные методы и средства анализа и управление рисками информационных систем компаний.
10.Правовые меры обеспечения информационной безопасности.
11.Организационные меры обеспечения безопасности компьютерных информационных систем.
12.Программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление доступом.
13.Протоколирование и аудит, шифрование, контроль целостности.

5.2. Темы письменных работ

1. В чем суть пентестирования по типу Белый ящик?
2. В чем суть пентестирования по типу Черный ящик?
3. В чем цель этапа пассивного тестирования - разведки?
4. В чем суть гарантированного уничтожения?
5. Какие характеристики сотрудников и почему косвенно могут указывать на них как на потенциальных злоумышленников или нарушителей политики обеспечения информационной безопасности?
6. Что такое ГосСОПКА?
7. Что такое SLA?
8. Какие применяются методы защиты информации от промышленного шпионажа?
9. Что понимается под объектом критической информационной инфраструктурой (КИИ) ?

10. Какие цели и задачи проведения тренингов по безопасности для сотрудников организации?
11. Как понятие эксплойт связано с информационной безопасностью?
12. В чем разница между такими документами как Регламент ИБ и Инструкция ИБ?
13. Что такое авторское право?
14. Какие варианты управления персоналом требуются для снижения инсайдерских угроз?
15. Каково содержание приказа ФСТЭК 21?
16. Что такое приказ ФСТЭК 17?
17. Какие требования предъявляются к руководителю службы безопасности банка?
18. Какие меры управления риском вы знаете?
19. Что понимается под управлением конфигурациями?
20. Что понимается под управлением обновлениями ПО?
21. Какие риски есть при применении продуктов Open Source?
22. Какова цель проведения аудита информационной безопасности?
23. Как определить эффективность работы СЗИ?
24. Кто и как устанавливает границы проведения аудита для оценки защищенности ИС от угроз ИБ?
25. Являются ли стандарты обязательными требованиями при выстраивании СУИБ?

5.3. Фонд оценочных средств

1. Защита от вредоносного программного обеспечения. Планирование систем и их приёмка.
2. Перечислите методы разграничения доступа в автоматизированных системах.
3. Что такое политика информационной безопасности автоматизированной системы?
4. По каким критериям относить автоматизированную систему к ГИС?
5. Раскройте понятие «аудит информационной безопасности».
6. Что такое SIEM-системы? Их назначение?
7. Что такое DLP-системы? Их назначение?
8. Что такое информационный актив?
9. Перечислите основные этапы разработки и функционирования СУИБ.
10. Перечислите основные процессы СУИБ.
11. Что такое ISMS?
12. Приведите примеры управленческих (организационных) мер защиты информации в автоматизированных системах.
13. Сколько классов защищенности АС Вы знаете? Примеры.
14. Является ли автоматизированная система объектом информатизации и почему?
15. Из каких основных подсистем строится система защиты информации в автоматизированной системе?
16. Сформулируйте причину(ы) привлечения к процессу анализа информационных рисков при автоматизированной обработке информации специалистов из различных подразделений компании?
17. Что такое «пентестинг»?
18. Раскройте понятие «частные политики ИБ».
19. Какие категории сведений, обрабатываемых в АС, можно отнести к сведениям конфиденциального характера (защищаемой информации)?
20. Сформулируйте цель обеспечения безопасности автоматизированной системы
21. Приведите примеры преднамеренных угроз информационной безопасности АС.
22. Приведите примеры непреднамеренных угроз информационной безопасности АС.
23. Какие методы аутентификации можно применять при защите АС?
24. В чем заключается дискреционный метод разграничения доступа?
25. Что такое модель PDCA в менеджменте информационной безопасности?
26. Раскройте термин «событие информационной безопасности».
27. С какого этапа необходимо начинать разработку системы информационной безопасности? Какие мероприятия могут быть заложены на данном этапе?
28. Что включает в себя комплексная система информационной безопасности?

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	Мельников В. П., под ред., Куприянов А. И.	Информационная безопасность: Учебник	Москва: КноРус, 2021, URL: https://book.ru/book/939292
Л1.2	Ищейнов В. Я.	Информационная безопасность и защита информации: словарь терминов и понятий: Словарь	Москва: Русайнс, 2021, URL: https://book.ru/book/938255

	Авторы, составители	Заглавие	Издательство, год
Л1.3	Николаев Н. С.	Управление информационной безопасностью: Учебник	Москва: КноРус, 2021, URL: https://book.ru/book/939841
6.1.2. Дополнительная литература			
	Авторы, составители	Заглавие	Издательство, год
Л2.1	Жукова М.Н., Жуков В.Г.	Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности: Учебное пособие	Красноярск: Федеральное государственное бюджетное образовательное учреждение высшего образования "Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева", 2012, URL: http://znanium.com/catalog/document?id=230373
Л2.2	Шилов А.К.	Управление информационной безопасностью: Учебное пособие	Ростов-на-Дону: Издательство Южного федерального университета (ЮФУ), 2018, URL: http://znanium.com/catalog/document?id=339855
Л2.3	Золотарев В.В., Данилова Е.А.	Управление информационной безопасностью. Ч. 1. Анализ информационных рисков: Практическое пособие	Красноярск: Федеральное государственное бюджетное образовательное учреждение высшего образования "Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева", 2010, URL: https://znanium.com/catalog/document?id=230365
Л2.4	Шилов А.К.	Управление информационной безопасностью: Учебное пособие	Ростов-на-Дону: Издательство Южного федерального университета (ЮФУ), 2018, URL: https://znanium.com/catalog/document?id=339855
6.2. Электронные учебные издания и электронные образовательные ресурсы			
Э1	Естественно-научный образовательный портал . - Режим доступа: http://www.en.edu.ru/		
Э2	Федеральный центр информационно-образовательных ресурсов. - Режим доступа: http://fcior.edu.ru/		
Э3	Интернет университет информационных технологий ИНТУИТ . - Режим доступа: https://www.intuit.ru/studies/courses		
Э4	Единое окно доступа к образовательным ресурсам . - Режим доступа: http://window.edu.ru		
Э5	Электронная библиотечная система Znanium. - Режим доступа: http://new.znanium.com/		
Э6	Электронные ресурсы Академии ИМСИТ . - Режим доступа: http://eios.imsit.ru/		
Э7	Web-ресурс «Официальный сайт Академии ИМСИТ . - Режим доступа: http://imsit.ru		
6.3.1. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства			
6.3.1.1	7-Zip Архиватор 7-Zip Программное обеспечение по лицензии GNU GPL		
6.3.1.2	Яндекс Браузер Браузер Яндекс Браузер Лицензионное соглашение на использование программ Яндекс Браузер https://yandex.ru/legal/browser_agreement/		
6.3.1.3	LibreOffice Офисный пакет LibreOffice Программное обеспечение по лицензии GNU GPL		
6.3.1.4	Windows 10 Pro RUS Операцинная система – Windows 10 Pro RUS Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2021		
6.3.1.5	Mozilla Firefox Браузер Mozilla Firefox Программное обеспечение по лицензии GNU GPL		

7. МТО (оборудование и технические средства обучения)			
Ауд	Наименование	ПО	Оснащение
123	Кабинет информационной безопасности	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. 1С:Предприятие 8. Комплект Kaspersky Endpoint Security MS Access 2016	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 Project Pro 2016 MS SQL Server 2019 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 Ramus Educational Micro-Cap Evaluation gvSIG Desktop Python	
235	Аудитория (защищаемое помещение) для проведения учебных занятий, с информацией ограниченного доступа, не содержащей сведений, составляющих государственную тайну	7-Zip Яндекс Браузер Mozilla Firefox LibreOffice	Стол – 8 шт., стул - 20 шт., рабочее место преподавателя – 1 шт., мультимедийный проектор (переносной) – 1 шт., переносной ноутбук – 1 шт., технические средства защиты
114а	Лаборатория программно-аппаратных средств защиты информации	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 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 PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclips	Стол - 20 шт., стул - 22 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., интерактивная доска WR-84A10 с проектором ViewSonic PS501X - 1 шт., соответствующее программное обеспечение Коммутатор LincSys SR224G – 1 шт., проектор ViewSonic PJD5232 – 1 шт., проекционный экран Luma – 1 шт., шкаф телекоммуникационный – 1 шт., ИБП SMART UPS 2000 – 1 шт., коммутатор Cisco Catalist 2960 – 3 шт., концентратор AlterPath 16 port – 1 шт., маршрутизатор Cisco-2800 – 4 шт., маршрутизатор Cisco-2811 – 2 шт., модуль 2-port – 6 шт., панель коммутационная 2 шт., Шнур V.35 Cable – 12 шт., витая пара, коннектор RJ-45, инструмент для зачистки кабеля UTP – 2 шт., протяжка кабельная, d=3,5 мм 10 м – 1 шт., тестер МЕГЕОН 40060/Шт. – 1 шт., инструмент для обжима витой пары – 5 шт., Тестер кабельный – 5 шт., инструмент для заделки кабеля витая пара тип Krone с крючками – 3 шт., Р телефон GrandStream GXP1610 – 2 шт., комплект для монтажа СКС (патч-панель 1U kat.5e UTP 24 порта-1 шт., инструмент обжимной для RJ-45 1 шт., инструмент для зачистки кабеля 1 шт., инструмент для разделки контактов - 1 шт., LAN тестер 1 шт.) – 2 шт., роутер Wi-Fi роутер Keenetic – 2 шт., сервер GA-870A-USB3/AMD-Phenom(tm)-II-X4-945/ DDR3-1333-4Гб/SSD Flexis 120Gb/WD5000AAKX/Radeon HD-5800/Realtek PCIe

		Adobe Reader DC NetBeans IDE ZEAL Klite Mega Codec Pack MS Office Standart 2010 Traffic inspector Special Unlimited Ramus Educational Micro-Cap Evaluation vGate Secren Net Studio Secren Net LSP Astra Linux Special Edition	GBE – 1 шт., аппаратные средства аутентификации пользователя: Соболь – 3 шт., эмуляторы активного сетевого оборудования в составе: Cisco Packet Tracer, Minine, Line Network Emulator, Marionnet – 21 шт., стенды для исследования параметров сетевого трафика в составе: WireShark, Snort, Colasoft Capsa Free, Ostinato, Suricata, Hping – 21 шт., средства антивирусной защиты: Kaspersky Endpoint Security для бизнеса, Dr.Web Security Space, средства защиты информации: ОС Astra Linux SE 1.7 «Смоленск» – 21 шт., Secret Net Studio – 21 шт., Secret Net LSP – 21 шт., vGate – 21 шт., стенд «Континент» – 21 шт., средства криптографической защиты информации: PGP – 21 шт., КриптоПро УЦ, – 21 шт., КриптоАРМ – 21 шт., КриптоПро CSP – 21 шт., межсетевые экраны: встроенные в ОС, стенд «Континент» – 21 шт., IPTables – 21 шт., Colasoft Capsa Free – 21 шт., средства обнаружения компьютерных атак: XSpider – 21 шт., MaxPatrol VM – 21 шт.
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 «Основы управления информационной безопасностью», 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 «Основы управления информационной безопасностью».
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