МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Юридический институт
Кафедра информационного права и информатики

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

КОРПОРАТИВНЫЕ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Кафедра информационного права и информатики
Юридического института

Образовательная программа
40.04.01 Юриспруденция

Направленность (профиль) программы
Информационное право и информационная безопасность

Уровень высшего образования
магистратура

Форма обучения
Очная, заочная

Статус дисциплины: **дисциплина по выбору**

Махачкала, 2021

Рабочая программа дисциплины «Корпоративные системы обеспечения информационной безопасности» составлена в 2021 году в соответствии с требованиями ФГОС ВО-магистратура по *направлению подготовки 40.04.01 Юриспруденция от 25 ноября 2020 года № 1451.*

Разработчик(и): кафедра «Информационного права и информатики»
Абдусаламов Руслан Абдусаламович, к.п.н., доцент,
Меджидова Хава Сайдалиевна, старший преподаватель.

Рабочая программа дисциплины одобрена:
на заседании кафедры информационного права и информатики
от «___» _____2021 г., протокол № __

Зав. кафедрой _____ Абдусаламов Р.А.

На заседании Методической комиссии юридического института
от «___» _____2021 г., протокол №___.

Председатель _____ Арсланбекова А.З.

Рабочая программа дисциплины согласована с учебно-методическим управлением «08» 07 _____2021 г.

Начальник УМУ_____ Гасангаджиева А.Г.

Аннотация рабочей программы дисциплины

Дисциплина «Корпоративные системы обеспечения информационной безопасности» является дисциплиной по выбору ОПОП магистратуры по направлению подготовки 40.04.01 «Юриспруденция».

Дисциплина реализуется в юридическом институте кафедрой информационного права и информатики.

Содержание дисциплины охватывает круг вопросов, связанных с разработкой политики безопасности организации и администрирования систем обеспечения информационной безопасности для решения задач в профессиональной деятельности Дисциплина нацелена на формирование следующих компетенций выпускника: общепрофессиональных – ОПК-7, профессиональных – ПК-4.

Преподавание дисциплины предусматривает проведение следующих видов учебных занятий: лекции, практические занятия, самостоятельная работа.

Рабочая программа дисциплины предусматривает проведение следующих видов контроля успеваемости в форме устного, письменного опроса и промежуточный контроль в форме зачета.

Объем дисциплины 2 зачетные единицы, в том числе 72 академических часа по видам учебных занятий:

Очная форма обучения

Семестр	Учебные занятия								Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен)
	в том числе:								
	всего	Контактная работа обучающихся с преподавателем						СРС, в том числе зачет	
		всего	из них						
			Лекции	Лабораторные занятия	Практические занятия	КСР	консультации		
3	72		8		2			62	зачет

Заочная форма обучения

Семестр	Учебные занятия								Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен)
	в том числе:								
	всего	Контактная работа обучающихся с преподавателем						СРС, в том числе зачет	
		всего	из них						
			Лекции	Лабораторные занятия	Практические занятия	КСР	консультации		
3	72		8		2			62	зачет

1. Цели освоения дисциплины

Целями освоения дисциплины «Корпоративные системы обеспечения информационной безопасности» являются овладение знаниями о функциональном составе корпоративных информационных систем, приобретение навыков работы с информацией и документами в рамках корпоративных информационных систем для решения профессиональных задач и с учетом требований информационной безопасности.

2.Место дисциплины в структуре ОПОП магистратуры

Дисциплина «Корпоративные системы обеспечения информационной безопасности» является дисциплиной по выбору ОПОП магистратуры по направлению подготовки 40.04.01 Юриспруденция, профиль «Информационное право и информационная безопасность».

Для полноценного усвоения дисциплины необходима предшествующая теоретическая подготовка по следующим дисциплинам: информационные технологии в юридической деятельности, информационное право, информационная безопасность.

Компетенции, полученные в результате освоения дисциплины «Корпоративные системы обеспечения информационной безопасности», необходимы обучающемуся при изучении следующих дисциплин:

- «Научно-исследовательская работа»;
- «Производственная практика»;
- «Преддипломная практика»;
- «Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы».

3. Компетенции обучающегося, формируемые в результате освоения дисциплины (перечень планируемых результатов обучения и процедура освоения).

Код и наименование компетенции из ОПОП	**Код и наименование индикатора достижения компетенций** *(в соответствии с ОПОП*	**Планируемые результаты обучения**	**Процедура освоения**
ОПК-7. Способен применять информационные технологии и использовать правовые базы данных для решения задач профессиональной деятельности с	ОПК-7.1. Получает из различных источников, включая правовые базы данных, юридически значимую информацию, обрабатывает и систематизирует ее в соответствии	Знает: информационные источники получения юридически значимой информации, включая профессиональные базы данных Умеет: получать из различных источников, включая правовые базы данных, юридически значимую информацию Владеет: навыками обработки	Письменный опрос …

учетом требований информационной безопасности	с поставленной целью	и систематизации информации в соответствии с поставленной целью	
	ОПК-7.2. Использует информацию, содержащуюся в отраслевых базах данных, для решения задач профессиональной деятельности	Знает: современные информационные технологии, которые используются в профессиональной деятельности юриста Умеет: решать задачи профессиональной деятельности с использованием информационных технологий Владеет: навыками применения профессиональных баз данных и информационных технологий в профессиональной деятельности	
	ОПК-7.3. Готов решать задачи профессиональной деятельности с учетом требований информационной безопасности	Знает: требования информационной безопасности в сфере своей профессиональной деятельности Умеет: решать задачи профессиональной деятельности с учетом требований информационной безопасности Владеет: навыками обеспечения информационной безопасности своей профессиональной деятельности	
ПК-4 Способен соблюдать в профессиональной деятельности требования правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	ПК-4.1 Способен понимать сущность и значение информации в развитии современного общества, соблюдать основные требования информационной безопасности, в т.ч. защиты государственной тайны	Знает: сущность и значение информации, содержащейся в служебной документации, основные требования режима секретности служебной документации Умеет: применять меры по обеспечению информационной безопасности Владеет: навыками засекречивания информации, обеспечения режима секретности	Круглый стол …
	ПК-4.2. Способен сознавать	Знает: виды угроз национальной безопасности	

	опасности и угрозы, возникающие в обществе	РФ, методы противодействия возникающим угрозам Умеет: выявлять признаки возникающих угроз национальной безопасности РФ, применять меры по предупреждению и пресечению возникших угроз Владеет: навыками борьбы и предупреждения возникающих угроз национальной безопасности РФ	
	ПК-4.3. Способен к выполнению должностных обязанностей по обеспечению законности и правопорядка, безопасности личности, общества, государства	Знает: должностные обязанности работников в области обеспечения законности и правопорядка Умеет: правильно исполнять их в своей профессиональной деятельности Владеет: методиками исполнения должностных обязанностей по обеспечению законности и правопорядка, безопасности личности, общества, государства; способен осуществлять профессиональную деятельность по обеспечению исполнения полномочий федеральных органов исполнительной власти, органов исполнительной власти субъектов РФ, лиц, замещающих государственные должности РФ, лиц, замещающих государственные должности субъектов РФ, и лиц, замещающих муниципальные должности, а также выполнять должностные обязанности по участию в осуществлении государственного контроля (надзора), муниципального контроля и общественного контроля.	

4. Объем, структура и содержание дисциплины.

4.1. Объем дисциплины составляет 2 зачетные единицы, 72 академических часа.

4.2. Структура дисциплины.

4.2.1. Структура дисциплины в очной форме

№ п/п	Разделы и темы дисциплины по модулям	Семестр	Виды учебной работы, включая самостоятельную работу студентов (в часах)					Формы текущего контроля успеваемости и промежуточной аттестации
			Лекции	Практические занятия	Лабораторные занятия	Консультации	Самостоятельная работа в т.ч. зачет	
Модуль 1. Политика информационной безопасности. Система управления информационной безопасностью								
1	Политика информационной безопасности.	3	2				16	Устный, письменный опрос
2	Управление и система управления информационной безопасностью	3	2				16	Устный, письменный опрос
	Итого по модулю 1:		4				32	
Модуль 2. Процессы проверки системы управления ИБ и оценка деятельности по управлению ИБ								
3	Оценка и управление рисками информационной безопасности	3	2				14	Устный, письменный опрос
4	Процессы проверки системы управления ИБ и оценка деятельности по управлению ИБ	3	2	2			12	Устный, письменный опрос
	Зачет						4	
	Итого по модулю 2:		4	2			32	
	ИТОГО:		8	2			62	зачет

4.2.2. Структура дисциплины в заочной форме

№ п/п	Разделы и темы дисциплины по модулям	Семестр	Виды учебной работы, включая самостоятельную работу студентов (в часах)					Формы текущего контроля успеваемости и промежуточной аттестации
			Лекции	Практические занятия	Лабораторные занятия	Консультации	Самостоятельная работа в т.ч. зачет	
Модуль 1. Политика информационной безопасности. Система управления информационной безопасностью								

1	Политика информационной безопасности.	3	2				16	Устный, письменный опрос
2	Управление и система управления информационной безопасностью	3	2				16	Устный, письменный опрос
	Итого по модулю 1:		4				32	
Модуль 2. Процессы проверки системы управления ИБ и оценка деятельности по управлению ИБ								
3	Оценка и управление рисками информационной безопасности	3	2				14	Устный, письменный опрос
4	Процессы проверки системы управления ИБ и оценка деятельности по управлению ИБ	3	2	2			12	Устный, письменный опрос
	Зачет						4	
	Итого по модулю 2:		4	2			32	
	ИТОГО:		8	2			62	зачет

4.3. Содержание дисциплины, структурированное по темам (разделам).

4.3.1. Содержание лекционных занятий по дисциплине.

Модуль 1. Политика информационной безопасности. Система управления информационной безопасностью

Тема 1. Политика информационной безопасности.

Понятия политики обеспечения ИБ и политики ИБ организации. Причины выработки политики ИБ. Основные требования и принципы, учитываемые при разработке и внедрении политики ИБ.

Содержание политики ИБ: содержание корпоративной политики ИБ, содержание частных политик ИБ, примеры частных политик ИБ.

Жизненный цикл политики ИБ: разработка политики ИБ, внедрение политики ИБ, применение политики ИБ, аннулирование политики ИБ, ответственность за исполнение политики ИБ.

Тема 2. Управление и система управления информационной безопасностью

Необходимость управления обеспечением ИБ организации. Деятельность по обеспечению ИБ организации как процесс. Определение управления ИБ организации. Управление ИБ информационно-телекоммуникационных технологий организации.

Система управления ИБ организации: область действия СУИБ, документальное обеспечение СУИБ, политика СУИБ, поддержка СУИБ со стороны руководства организации.

Процессный подход в рамках управления ИБ: планирование СУИБ, реализация СУИБ, проверка СУИБ, совершенствование СУИБ.

Работа с процессами СУИБ организации: задание процесса СУИБ, идентификация процессов СУИБ организации, документирование и описание процесса СУИБ, мониторинг и измерение параметров процесса СУИБ.

Стратегии построении и внедрения СУИБ: построение и внедрение СУИБ в целом, построение и внедрение процессов СУИБ по отдельности

Модуль 2. Политика информационной безопасности. Система управления информационной безопасностью

Тема 3. Оценка и управление рисками информационной безопасности

Основные определения. Нормативное обеспечение управления рисками информационной безопасности. Оценка рисков информационной безопасности. Обработка рисков информационной безопасности. Принятие и мониторинг рисков информационной безопасности. Обеспечение управления рисками информационной безопасности.

Тема 4. Процессы проверки системы управления ИБ и оценка деятельности по управлению ИБ

Нормативное обеспечение проверки и оценки деятельности по управлению информационной безопасностью.

Аудит СУИБ. Процесс аудита. Внутренний и внешний аудит. Аудит первой, второй и третьей сторонами. Подготовка к выполнению аудита. Подготовка и представление отчетов в устной и письменной форме о результатах аудита. Принятие решений о необходимости соответствующих последующих аудиторских проверок.

Оценка деятельности по управлению информационной безопасностью.

4.3.2. Содержание практических занятий по дисциплине.

Система управления ИБ организации: область действия СУИБ, документальное обеспечение СУИБ, политика СУИБ, поддержка СУИБ со стороны руководства организации.

Стратегии построении и внедрения СУИБ: построение и внедрение СУИБ в целом, построение и внедрение процессов СУИБ по отдельности

Нормативное обеспечение проверки и оценки деятельности по управлению информационной безопасностью.

Аудит СУИБ. Процесс аудита. Внутренний и внешний аудит. Аудит первой, второй и третьей сторонами. Подготовка к выполнению аудита. Подготовка и представление отчетов в устной и письменной форме о результатах аудита. Принятие решений о необходимости соответствующих последующих аудиторских проверок.

Оценка деятельности по управлению информационной безопасностью.

5. Образовательные технологии

В соответствии с требованиями ФГОС ВО по направлению подготовки Юриспруденция в рамках изучения данной дисциплины для реализации компетентностного подхода предусмотрено все проводимые занятия, в том числе самостоятельная работа магистранта, сочетать передовые методические приемы с новыми образовательными информационными технологиями и достижениями науки и техники.

№ п/п	Вид учебной работы	Образовательные технологии
1.	Лекции	• Лекция-информация с визуализацией • Проблемная лекция
2.	Практические занятия	• Семинар-дискуссия, семинар-дебаты по актуальным проблемам интернет-права • Выполнение практических работ • Решение проблемных ситуаций из области интернет-права • Семинар-конференция по студенческим докладам и эссе • Имитационные (ситуативные) технологии • Проектные технологии • Ролевые игры • Технология учебного исследования
3.	Самостоятельная работа	• Письменные и устные домашние задания • Консультации преподавателя • Поиск и анализ информации в справочных правовых системах и сети Интернет • Внеаудиторная работа студентов (освоение теоретического материала, подготовка к семинарским занятиям, выполнение домашних заданий, выполнение творческой работы, работа с электронным учебно-методическим комплексом, подготовка к текущему и итоговому контролю)
4.	Контроль	• Выступление на семинарах • Выполнение практических заданий • Защита рефератов • Устный опрос • Письменный опрос

В учебном процессе при реализации компетентностного подхода используются лекционные и практические занятия, в том числе в форме активных и интерактивных форм проведения занятий: деловые и ролевые игры, разбор конкретных юридических ситуаций. Эти формы сочетаются с самостоятельной работой студента в целях закрепления и развития полученных знаний. Возможно проведение встреч с представителями правозащитных организаций, избирательных комиссий разного уровня, привлечение иностранных специалистов, профессоров и др.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью (миссией) программы, особенностью контингента обучающихся и содержанием конкретных дисциплин. Занятия лекционного типа для соответствующих групп студентов не могут составлять более 20% аудиторных занятий.

Для студентов с ограниченными возможностями здоровья предусмотрены следующие формы организации педагогического процесса и контроля знаний:

- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- для выполнения контрольных заданий при необходимости предоставляется увеличивающее устройство;
- задания для выполнения, а также инструкция о порядке выполнения контрольных заданий оформляются увеличенным шрифтом (размер 16-20);
- для глухих и слабослышащих:
- обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости студенту предоставляется звукоусиливающая аппаратура индивидуального пользования;
- для лиц с тяжелыми нарушениями речи, глухих, слабослышащих все контрольные задания по желанию студентов могут проводиться в письменной форме.

Основной формой организации педагогического процесса является интегрированное обучение инвалидов, т.е. все студенты обучаются в смешанных группах, имеют возможность постоянно общаться со сверстниками, легче адаптируются в социуме.

6. Учебно-методическое обеспечение самостоятельной работы студентов.

Самостоятельная работа – вид индивидуальной деятельности магистранта, основанный на собственных познавательных ресурсах. Целью самостоятельной работы магистрантов является обучение навыкам работы с

научной литературой и практическими материалами, необходимыми для углубленного изучения курса наследственного права, а также развитие у них устойчивых способностей к самостоятельному (без помощи преподавателя) изучению и изложению полученной информации. В связи с этим основными задачами самостоятельной работы магистрантов, изучающих дисциплину «Корпоративные системы обеспечения информационной безопасности» являются:

- во-первых, продолжение изучения дисциплины в домашних условиях по программе, предложенной преподавателем;
- во-вторых, привитие магистрантам интереса к юридической литературе, правотворческому процессу.

Изучение и изложение информации, полученной в результате изучения научной литературы и практических материалов, предполагает развитие у магистрантов как владения навыками устной речи, так и способностей к четкому письменному изложению материала.

Виды и порядок выполнения самостоятельной работы:

№ п/п	Вид самостоятельной работы	Вид контроля
1.	Подготовка реферата, презентации и доклада.	Прием реферата, презентации, доклада и оценка качества их исполнения на мини-конференции
2.	Освоение теоретического материала	Устный и письменный опрос
3.	Подготовка к практическим занятиям	Практические задания

Нормативные акты

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ).

2. Концепция государственной информационной политики РФ, одобренная Комитетом Государственной Думы по информационной политике и связи 15.10.1998.

3. Федеральный закон от 13.01.1995 № 7-ФЗ (ред. от 12.03.2014) «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации».

4. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 04.06.2014) «О персональных данных».

5. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 19.12.2016) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.01.2017).

6. Федеральный закон от 22.12.2008 N 262-ФЗ (ред. от 23.06.2016) "Об обеспечении доступа к информации о деятельности судов в Российской Федерации" / "Российская газета", N 265, 26.12.2008.

7. Федеральный закон от 09.02.2009 N 8-ФЗ (ред. от 09.03.2016) "Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления".

8. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ (ред. от 12.03.2014).

9. Указ Президента РФ от 28.06.1993 N 966 (ред. от 22.03.2005) "О Концепции правовой информатизации России" // Собрание актов Президента и Правительства РФ. 05.07.1993. N27. ст. 2521.

10. Указ Президента РФ от 20.01.1994 N 170 (ред. от 09.07.1997) "Об основах государственной политики в сфере информатизации" // Собрание актов Президента и Правительства РФ. 24.01.1994. N 4. Указ Президента РФ от 30.06.2012 N 918 "Об Управлении Президента Российской Федерации по применению информационных технологий и развитию электронной демократии".

11. Указ Президента РФ от 21.08.2012 N 1202 (ред. от 25.07.2014) "Об утверждении Положения об Управлении Президента Российской Федерации по применению информационных технологий и развитию электронной демократии".

12. Указ Президента РФ от 09.05.2017 N 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы".

13. Указ Президента РФ от 04.03.2013 N 183 (ред. от 23.06.2014) "О рассмотрении общественных инициатив, направленных гражданами Российской Федерации с использованием Интернет-ресурса "Российская общественная инициатива" (вместе с "Правилами рассмотрения общественных инициатив, направленных гражданами Российской Федерации с использованием Интернет-ресурса "Российская общественная инициатива").

14. Постановление Правительства РФ от 03.11.1994 № 1233 (ред. от 20.07.2012) «Об утверждении Положения о порядке обращения со служебной

информацией ограниченного распространения в федеральных органах исполнительной власти».

15. Постановление Правительства РФ от 24.05.2010 N 365 (ред. от 05.05.2016) "О координации мероприятий по использованию информационно-коммуникационных технологий в деятельности государственных органов" // Собрание законодательства РФ. 31.05.2010. N22, ст. 2778.

7. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

7.1. Типовые контрольные задания

Примерная тематика рефератов (творческих работ)

1. Серия стандартов ISO/IEC 27000 «Информационные технологии. Методы обеспечения безопасности».
2. Стандарты на отдельные процессы управлении ИБ и оценку безопасности ИТ: ISO/IEC 13335 - методы и средства обеспечения безопасности информационных технологий, ISO/IEC 15408 и ISO/IEC 18045 - Общие критерии и методология оценки безопасности информационных технологий, ISO 19011:2018 и ГОСТ Р ИСО 19011-2012 - Рекомендации по аудиту систем менеджмента, BS 25999 и ГОСТ Р 53647 - Управление непрерывностью бизнеса.
3. Законы о Банке Росии - Федеральный закон от 10 июля 2002 г. N 86-ФЗ "О Центральном банке Российской Федерации (Банке России)" и Федеральный закон от 27 июня 2011 г. N 161-ФЗ «О национальной платежной системе».
4. ГОСТ Р 57580.1-2017 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер (уровни защиты). ГОСТ Р 57580.2-2018 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия (оценка соответствия уровней защиты).
5. Отраслевые стандарты в области управления ИБ - стандарты Банка России, рекомендации Банка России и положения Банка России по защите информации.
6. Нормативная база управления инцидентами ИБ и обеспечение непрерывности бизнеса. Стандарт ISO 27035. Идентификация, протоколирование, реагирование на инциденты ИБ. Влияние инцидентов ИБ

на бизнес-процессы.

7. Средства управления событиями ИБ. SOC-центры ИБ, SIEM-системы управления информацией о безопасности и событиями информационной безопасности, IRP-системы автоматизации реагирования на инциденты информационной безопасности

8. Управление непрерывностью бизнеса организации.

Вопросы к зачету

1. Система. Системный подход. Процесс. Процессный подход. Управление. Циклическая модель улучшения процессов. Системный подход к управлению организацией. Процессный подход к управлению организацией. Информационная безопасность.

2. Понятия политики обеспечения ИБ и политики ИБ организации. Причины выработки политики ИБ. Основные требования и принципы, учитываемые при разработке и внедрении политики ИБ.

3. Содержание политики ИБ: содержание корпоративной политики ИБ, содержание частных политик ИБ, примеры частных политик ИБ.

4. Жизненный цикл политики ИБ: разработка политики ИБ, внедрение политики ИБ, применение политики ИБ, аннулирование политики ИБ, ответственность за исполнение политики ИБ.

5. Необходимость управления обеспечением ИБ организации. Деятельность по обеспечению ИБ организации как процесс. Определение управления ИБ организации. Управление ИБ информационно-телекоммуникационных технологий организации.

6. Система управления ИБ организации: область действия СУИБ, документальное обеспечение СУИБ, политика СУИБ, поддержка СУИБ со стороны руководства организации.

7. Процессный подход в рамках управления ИБ: планирование СУИБ, реализация СУИБ, проверка СУИБ, совершенствование СУИБ.

8. Работа с процессами СУИБ организации: задание процесса СУИБ, идентификация процессов СУИБ организации, документирование и описание процесса СУИБ, мониторинг и измерение параметров процесса СУИБ.

9. Стратегии построении и внедрения СУИБ: построение и внедрение СУИБ в целом, построение и внедрение процессов СУИБ по отдельности.

10. Основные определения. Нормативное обеспечение управления рисками информационной безопасности.

11. Оценка рисков информационной безопасности.

12. Обработка рисков информационной безопасности.

13. Принятие и мониторинг рисков информационной безопасности.

14. Обеспечение управления рисками информационной безопасности.

15. Нормативная база управления инцидентами ИБ и обеспечение непрерывности бизнеса. Стандарт ISO 27035. Идентификация, протоколирование, реагирование на инциденты ИБ. Влияние инцидентов ИБ на бизнес-процессы.

16. Средства управления событиями ИБ. SOC-центры ИБ, SIEM-системы управления информацией о безопасности и событиями информационной безопасности, IRP-системы автоматизации реагирования на инциденты информационной безопасности

17. Управление непрерывностью бизнеса организации.

18. Нормативное обеспечение проверки и оценки деятельности по управлению информационной безопасностью.

19. Аудит СУИБ. Процесс аудита. Внутренний и внешний аудит. Аудит первой, второй и третьей сторонами. Подготовка к выполнению аудита. Подготовка и представление отчетов в устной и письменной форме о результатах аудита. Принятие решений о необходимости соответствующих последующих аудиторских проверок.

20. Оценка деятельности по управлению информационной безопасностью.

7.2. Критерии оценивания.

Общий результат выводится как интегральная оценка, складывающая из текущего контроля - 70% и промежуточного контроля - 30%.

Текущий контроль по дисциплине включает:

- посещение занятий – 5 баллов,
- наличие конспектов – 5 баллов,
- участие на практических занятиях - 30 баллов,
- самостоятельная работа - 30 баллов.

Промежуточный контроль по дисциплине включает:

- коллоквиум - 15 баллов,
- письменная контрольная работа - 15 баллов.

8. Учебно-методическое обеспечение дисциплины.

а) основная литература:

1. Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс]: лабораторный практикум / М.А. Лапина [и др.]. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 242 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/62945.html

2. Пелешенко В.С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления [Электронный ресурс]: учебное пособие / В.С. Пелешенко, С.В. Говорова, М.А. Лапина. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2017. — 86 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/69405.html

3. Информационная безопасность при управлении техническими системами [Электронный ресурс]: учебное пособие / С.Ф. Баркалов [и др.]. — Электрон. текстовые данные. — СПб.: Интермедия, 2017. — 528 с. — 978-5-4383-0133-2. — Режим доступа: http://www.iprbookshop.ru/68589.html

4. Программно-аппаратные средства защиты информации [Электронный ресурс]: учебное пособие для студентов вузов по направлению подготовки «Информационная безопасность» / Л.Х. Мифтахова [и др.] – Электрон. текстовые данные. – СПб.: Интермедия, 2018 – 408 с. – 978-5-4383-0157-8. – Режим доступа: http://www.iprbookshop.ru/736443.html

б) дополнительная литература:

1. Анисимов А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс] / А.А. Анисимов. — Электрон. текстовые данные. — М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 212 с. — 978-5-9963-0237-6. — Режим доступа: http://www.iprbookshop.ru/52182.html

2. Сычев Ю.Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов [Электронный ресурс] : учебное пособие / Ю.Н. Сычев. — Электрон. текстовые данные. — Саратов: Вузовское образование, 2018. — 195 с. — 978-5-4487-0128-3. — Режим доступа: http://www.iprbookshop.ru/72345.html

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.

1. Научная электронная библиотека: elibrary.ru
2. Федеральный портал «Российское образование»: www.edu.ru/
3. Федеральное хранилище «Единая коллекция цифровых образовательных ресурсов»: http://school-collection.edu.ru/
4. Российский портал «Открытого образования»: www.openet.edu.ru
5. Сайт образовательных ресурсов Даггосуниверситета: edu.icc.dgu.ru
6. Информационные ресурсы научной библиотеки Даггосуниверситета elib.dgu.ru (доступ через платформу Научной электронной библиотеки elibrary.ru).
7. Федеральный центр образовательного законодательства. www.lexed.ru.
8. Библиотека и форум по программированию. URL: http://www.cyberforum.ru

9. Национальный открытый университет ИНТУИТ. URL: http://www.intuit.ru/

10. Открытая электронная библиотека: www.diss.rsl.ru.

11. Все о праве: www.allpravo.ru.

12. Юридическая литература по праву: www.okpravo.info.

13. Юридический портал "Правопорядок": www.oprave.ru.

14. СПС «Гарант»: www.garant.ru.

15. СПС «Консультант плюс»: www.tls-cons.ru.

16. СПС «Право»: www.pravo.ru.

10. Методические указания для обучающихся по освоению дисциплины.

Успешное изучение дисциплины требует посещения лекций, активной работы на лабораторных работах и практических занятиях, выполнения всех учебных заданий преподавателя, ознакомления с основной и дополнительной литературой в рамках самостоятельной работы.

Рекомендуется следующим образом организовать время, необходимое для изучения дисциплины:

- посещение всех лекции и практических занятий;

- изучение конспекта лекции в тот же день, после лекции (10 – 15 минут);

- изучение конспекта лекции за день перед следующей лекцией (10 – 15 минут);

- изучение теоретического материала по учебнику и конспекту (1 час в неделю);

- прежде чем посетить следующую лекцию, добейтесь того, чтобы вам было полностью понятно содержание всего предыдущего материала;

- работайте регулярно, не накапливайте не понятое и не сданное.

Кроме чтения учебной литературы из обязательного списка рекомендуется активно использовать информационные ресурсы сети Интернет по изучаемой теме.

Самостоятельное изучение тем дисциплины способствует:

- закреплению знаний, умений и навыков, полученных в ходе аудиторных занятий;

- углублению и расширению знаний по отдельным вопросам и темам дисциплины.

Самостоятельная работа как вид учебной работы может использоваться на лекциях, а также иметь самостоятельное значение – внеаудиторная самостоятельная работа обучающихся – при подготовке к зачету.

Основными видами самостоятельной работы по дисциплине являются:

- изучение конспектов лекций при подготовке к практическим занятиям, и при подготовке к зачету;

- самостоятельное изучение отдельных вопросов дисциплины с применением учебников и дополнительной литературы.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем.

При осуществлении образовательного процесса по дисциплине «Корпоративные системы обеспечения информационной безопасности»используются следующие информационные технологии:

1. **Презентации** – это электронные диафильмы, которые могут включать в себя анимацию, аудио- и видеофрагменты, элементы интерактивности. Презентации активно используются и для представления ученических проектов.
2. **Электронные энциклопедии** поддерживают удобную систему поиска по ключевым словам и понятиям.
3. **Дидактические материалы** – сборники задач, а также примеров рефератов, представленных в электронном виде.
4. **Электронные учебники и учебные курсы.**

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

- Аудиторный класс.
- Компьютерный класс.
  Ноутбук, мультимедиа проектор