Федеральное государственное бюджетное образовательное учреждение высшего образования

САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АРХИТЕКТУРНО-СТРОИТЕЛЬНЫЙ УНИВЕРСИТЕТ

Кафедра Экономической безопасности

УТВЕРЖДАЮ
Начальник учебно-методического управления
Михайлова Анна Олеговна
Подписано цифровой подписью: Михайлова Анна Олеговна
«29» июня 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Анализ и оценка информационной составляющей экономической безопасности

направление подготовки/специальность 38.05.01 Экономическая безопасность

направленность (профиль)/специализация образовательной программы Финансово-аналитическое обеспечение экономической безопасности хозяйствующих субъектов и организаций

Форма обучения очная

Санкт-Петербург, 2023

1. Цели и задачи освоения дисциплины (модуля)

1. Изучить действующие нормативно-правовые документы в области защиты информационных активов предприятия и персональных данных.

2. Получить базовые знания в области защиты данных в информационных системах.

3. Получить первичные навыки по использованию специализированного программного обеспечения для защиты информационных активов и решения профессиональных задач в области экономической безопасности.

1. Изучение источников угроз информационной безопасности. Место рисков информационной безопасности в структуре рисков бизнеса.

2. Изучение требований стандартов и нормативных документов в области информационной безопасности.

3. Изучение основных видов систем информационной безопасности и способов защиты.

4. Знакомство с возможностями использования программных продуктов информационной безопасности для решения задач экономической безопасности.

5. Изучение функционала DLP-систем.

6. Получение навыков использования DLP-систем для решения задач информационной и экономической безопасности.

7. Изучение организационных аспектов информационной безопасности.

8. Знакомство с системами защиты электронного документооборота.

2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов освоения ОПОП
ПК-3 Способен проводить экономический анализ деятельности организации	ПК-3.1 Проводит сбор и обработку данных для проведения расчетов экономических показателей организации	**знает** Законодательную и нормативную базу в области обеспечения информационной безопасности и соблюдения режима секретности. Состав затрат на внедрение и эксплуатацию информационных систем, включая системы информационной безопасности. Возможности DLP-систем по: - сбору "цифрового следа" использования рабочего времени сотрудниками; - сбору данных о нарушениях политики конфиденциальности организации (защита информационных активов); - сбору данных об отклонениях в реализации текущих бизнес-процессов организации. **умеет** - устанавливать параметры DLP-системы; - собрать и классифицировать информацию о критических информационных активах и местах их хранения. **владеет** - навыком построения фильтров и отчетов DLP-системы.

ПК-3 Способен проводить экономический анализ деятельности организации	ПК-3.2 Осуществляет расчет экономических показателей результатов деятельности организации	**знает** - методы расчета экономической эффективности информационных систем и систем информационной безопасности; - способы контроля реализации бизнес-процессов в организации и соответствующие показатели. **умеет** - рассчитывать текущую стоимость владения системой безопасности; - рассчитывать показатели экономической эффективности инвестиционного проекта внедрения системы информационной безопасности. **владеет** - навыком расчета затрат на приобретение и эксплуатацию системы информационной (экономической) безопасности; - навыком использования юридически значимой информации, содержащейся в массивах учетов, с целью ведения профессиональной деятельности.
ПК-3 Способен проводить экономический анализ деятельности организации	ПК-3.3 Проводит оценку показателей экономической безопасности организации в соответствии с поставленной задачей	**знает** - критерии оценки системы информационной безопасности организации по российским и международным стандартам; - актуальные риски информационной безопасности. **умеет** - выявлять риски нарушения бизнес-процессов, корпоративной этики, коррупционных и других нарушений с использованием DLP-систем; - делать выводы о результативности организационных мер по обеспечению безопасности (информационной, экономической). **владеет** - навыком выбора системы информационной безопасности из нескольких альтернатив по результатам расчета показателей эффективности инвестиционного проекта и (или) текущей стоимости владения.

ПК-3 Способен проводить экономический анализ деятельности организации	ПК-3.4 Составляет отчет по результатам экономического анализа деятельности организации	**знает** - структуру отчета по результатам аудита информационной безопасности; - критерии определения уровня зрелости организации в области информационной безопасности. **умеет** - анализировать и выбирать адекватные модели информационной безопасности, планировать их реализацию на базе требований к современному уровню защиты тайны и информационной безопасности, соблюдению режима секретности - делать выводы о наличии (отсутствии) подозрительных действий, перемещения документов по данным DLP-системы. **владеет** - навыком анализа процессов организации с целью выявления возможной утраты ресурсов организации; - навыком проведения расследования инцидента на основе данных DLP-системы.

ПК-3 Способен проводить экономический анализ деятельности организации	ПК-3.5 Составляет рекомендации по улучшению экономических показателей организации	**знает** - основные меры, направленные на обеспечение информационной безопасности, соблюдение режима секретности на различных уровнях деятельности - оформлять соответствующую документацию для обеспечения функционирования информационных массивов; - теоретические основы по управлению операционными рисками; - назначение основных классов систем информационной безопасности. **умеет** - разрабатывать рекомендации по устранению ошибок в деятельности, связанных с информационной безопасностью, обеспечением соблюдения режима секретности; - обоснованно выбирать и рекомендовать использование систем безопасности определенного назначения (SIEM, DLP, системы криптографической защиты, IRP, др.), исходя из выявленных рисков информационной (экономической) безопасности. **владеет** - навыком использования отчетов DLP-системы по учету использования рабочего времени для разработки предложений по оптимизации бизнес-процессов; - навыком организации обучения сотрудников вопросам информационной безопасности; - навыком разработки политики информационной безопасности.

3. Указание места дисциплины (модуля) в структуре образовательной программы

Данная дисциплина (модуль) включена в Блок «Дисциплины, модули» Б1.В.03 основной профессиональной образовательной программы 38.05.01 Экономическая безопасность и относится к части, формируемой участниками образовательных отношений учебного плана.

№ п/п	Предшествующие дисциплины	Код и наименование индикатора достижения компетенции
1	Гражданское право	ОПК-5.1, ОПК-5.2
2	Организация системы экономической безопасности	ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2
3	Цифровая экономика и безопасность	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК -3.1, ОПК-3.2, ПК(Ц)-1.1, ПК(Ц)-1.2, ОПК-6.1, ОПК-6.2
4	Экономическая безопасность	ОПК-3.1, ОПК-3.2, ОПК-6.1, ОПК -6.2, ПК(Ц)-1.1, ПК(Ц)-1.2
5	Информационные технологии	УК-1.1, УК-1.2, УК-1.6, ОПК-7.1, ОПК-7.2, ОПК-7.3

6	Специализированное программное обеспечение экономической безопасности	ПК-1.1, ПК-2.1, ПК(Ц)-1.1, ПК(Ц)-1.2

Гражданское право

знать нормы права и нормы профессиональной этики, исключающие неправомерное использование работодателем специализированных систем информационной безопасности

Организация системы экономической безопасности

умеет провести анализ комплексной системы экономической безопасности организации

Цифровая экономика и безопасность

умеет выявлять внутренние и внешние угрозы и риски с целью их предупреждения, локализации или нейтрализации

Экономическая безопасность

знает основы организации системы безопасности хозяйствующего субъекта

Информационные технологии

владеет навыком поиска информационных ресурсов, сбора и обработки информации о проблемной ситуации

Специализированное программное обеспечение экономической безопасности

знает теоретические основы организации мониторинга деятельности персонала организации с помощью DLP-систем

знает назначение криптографических средств защиты и понимает необходимость использования механизмов защиты при разработке технологических карт электронного документооборота

№ п/п	Последующие дисциплины	Код и наименование индикатора достижения компетенции
1	Практика по экономической и информационной безопасности. Часть 1	УК-9.1, УК-9.2, УК-9.3, УК-10.1, УК-10.2, УК-10.3, УК-10.4, УК-10.5, ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК-2.4, ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4, ПК-3.5, ПК-4.1, ПК-4.2, ПК-4.3, ПК-4.4, ПК-4.5, ПК-5.1, ПК-5.2, ПК-5.3, ПК-5.4, ПК(Ц)-1.1, ПК(Ц)-1.2
2	Конкурентная разведка	ПК-2.1, ПК-2.2, ПК-2.3, ПК-2.4
3	Практика по экономической и информационной безопасности. Часть 2	УК-9.1, УК-9.2, УК-9.3, УК-10.1, УК-10.2, УК-10.3, УК-10.4, УК-10.5, ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК-2.4, ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4, ПК-3.5, ПК-4.1, ПК-4.2, ПК-4.3, ПК-4.4, ПК-4.5, ПК-5.1, ПК-5.2, ПК-5.3, ПК-5.4, ПК(Ц)-1.1, ПК(Ц)-1.2

4	Преддипломная практика	УК-1.1, УК-1.2, УК-1.3, УК-1.4, УК-1.5, УК-1.6, УК-2.1, УК-2.2, УК-2.3, УК-2.4, УК-2.5, УК-3.1, УК-3.2, УК-3.3, УК-3.4, УК-4.1, УК-4.2, УК-4.3, УК-4.4, УК-6.1, УК-6.2, УК-6.3, УК-7.1, УК-7.2, УК-7.3, УК-7.4, УК-8.1, УК-8.2, УК-8.3, УК-8.4, УК-9.1, УК-9.2, УК-9.3, УК-10.1, УК-10.2, УК-10.3, УК-10.4, УК-10.5, УК-11.1, УК-11.2, УК-11.3, ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК-2.4, ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4, ПК-3.5, ПК-4.1, ПК-4.2, ПК-4.3, ПК-4.4, ПК-4.5, ПК-5.1, ПК-5.2, ПК-5.3, ПК-5.4, ПК(Ц)-1.1, ПК (Ц)-1.2
5	Управление проектами и безопасность бизнес-процессов	ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4, ПК-3.5, ПК-4.1, ПК-4.2, ПК-4.3, ПК-4.4, ПК-4.5
6	Подготовка к процедуре защиты и защита выпускной квалификационной работы	УК-1.1, УК-1.2, УК-1.3, УК-1.4, УК-1.5, УК-1.6, УК-2.1, УК-2.2, УК-2.3, УК-2.4, УК-2.5, УК-3.1, УК-3.2, УК-3.3, УК-3.4, УК-4.1, УК-4.2, УК-4.3, УК-4.4, УК-6.1, УК-6.2, УК-6.3, УК-7.1, УК-7.2, УК-7.3, УК-7.4, УК-8.1, УК-8.2, УК-8.3, УК-8.4, УК-9.1, УК-9.2, УК-9.3, УК-10.1, УК-10.2, УК-10.3, УК-10.4, УК-10.5, УК-11.1, УК-11.2, УК-11.3, ОПК-1.1, ОПК-1.2, ОПК-1.3, ОПК-1.4, ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-4.1, ОПК-4.2, ОПК-4.3, ОПК-5.1, ОПК-5.2, ОПК-6.1, ОПК-6.2, ОПК-7.1, ОПК-7.2, ОПК-7.3, ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК-2.4, ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4, ПК-3.5, ПК-4.1, ПК-4.2, ПК-4.3, ПК-4.4, ПК-4.5, ПК-5.1, ПК-5.2, ПК-5.3, ПК-5.4, ПК(Ц)-1.1, ПК(Ц)-1.2, УК-5.1, УК-5.2, УК-5.3, УК-5.4, УК-5.5, УК-5.6

4. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Вид учебной работы	Всего часов	Из них часы на практическую подготовку	Семестр		
			4	5	6
Контактная работа	144		48	48	48
Лекционные занятия (Лек)	48	0	16	16	16
Практические занятия (Пр)	96	96	32	32	32
Иная контактная работа, в том числе:	1,5				1,5
консультации по курсовой работе (проекту), контрольным работам (РГР)	1				1
контактная работа на аттестацию (сдача зачета, зачета с оценкой; защита курсовой работы (проекта); сдача контрольных работ (РГР))	0,25				0,25
контактная работа на аттестацию в сессию (консультация перед экзаменом и сдача	0,25				0,25
Часы на контроль	34,75		4	4	26,75
Самостоятельная работа (СР)	179,75		56	56	67,75
Общая трудоемкость дисциплины (модуля)					
часы:	360		108	108	144
зачетные единицы:	10		3	3	4

5. Содержание дисциплины (модуля), структурированное по разделам (темам) с указанием отведенного на них количества академических часов и видов учебных занятий

5.1. Тематический план дисциплины (модуля)

№	Разделы дисциплины	Семестр	Контактная работа (по учебным занятиям), час.						СР	Всего, час.	Код индикатора достижения компетенции
			лекции		ПЗ		ЛР				
			всего	из них на практическую подготовку	всего	из них на практическую подготовку	всего	из них на практическую подготовку			
1.	1 раздел. Безопасность в цифровой экономике и информационное законодательство										
1.1.	Информация. Информационное право.	4	3		12	12			4	19	ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4, ПК-3.5
1.2.	Правовые режимы доступа к информации. Безопасность в цифровой экономике	4	5		4	4			16	25	ПК-3.3, ПК-3.4, ПК-3.5
2.	2 раздел. Правовое регулирование в информационное сфере										
2.1.	Безопасность и регулирование электронного документооборота и массового распространения информации	4	4		8	8			18	30	ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4, ПК-3.5
2.2.	Информационная безопасность РФ на национальном уровне	4	4		8	8			18	30	ПК-3.3, ПК-3.4, ПК-3.5
3.	3 раздел. Контроль										
3.1.	Зачёт	4								4	ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4, ПК-3.5
4.	4 раздел. Теоретические основы управления информационной безопасностью бизнеса										
4.1.	Информация и бизнес. Информационная безопасность	5	4		12	12			18	34	ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4, ПК-3.5
4.2.	Управление информационной безопасностью бизнеса	5	6		4	4			5	15	ПК-3.3, ПК-3.5

5.	5 раздел. Общая характеристика систем и средств обеспечения информационной безопасности										
5.1.	Обзор основных средств обеспечения информационной безопасности	5	4		8	8			8	20	ПК-3.3, ПК-3.5
5.2.	Документальное обеспечение информационной безопасности	5	2		8	8			25	35	ПК-3.3, ПК-3.5
6.	6 раздел. Контроль										
6.1.	Зачёт	5								4	ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4, ПК-3.5
7.	7 раздел. Специализированные системы информационной безопасности										
7.1.	Криптография как основа защиты данных при хранении и передаче по каналам связи	6	2		8	8			27,75	37,75	ПК-3.3
7.2.	Системы защиты данных от утечек	6	6		8	8			5	19	ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4, ПК-3.5
8.	8 раздел. Мониторинг инцидентов информационной безопасности. Оценка системы информационной безопасности организации										
8.1.	Стандарты информационной безопасности	6	4		8	8			20	32	ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4, ПК-3.5
8.2.	Работа с инцидентами информационной безопасности. Платформа реагирования на инциденты (IRP). Security Operational Center (SOC)	6	4		8	8			15	27	ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4, ПК-3.5
9.	9 раздел. Иная контактная работа										

9.1.	Иная контактная работа	6								1,25	ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4, ПК-3.5
10.	10 раздел. Контроль										
10.1.	Экзамен	6								27	ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4, ПК-3.5

5.1. Лекции

№ разд	Наименование раздела и темы лекций	Наименование и краткое содержание лекций
1	Информация. Информационное право.	Система информационного права Понятие информации. Виды информации. Юридически значимые свойства информации. Информационное общество. Окинавская хартия глобального информационного общества. Единое информационное пространство. Система информационного права.
1	Информация. Информационное право.	Информационные правоотношения Субъекты и объекты, содержание информационных правоотношений
2	Правовые режимы доступа к информации. Безопасность в цифровой экономике	Правовые основы защиты конфиденциальных данных Документированная и недокументированная информация. Понятие и виды документов. Носители документированной информации. Документы на бумажных носителях. Понятие электронного документа. Электронная подпись и ее виды. Принципы и условия использования электронной подписи. Правовой режим информации, размещаемой в сети «Интернет». Законодательство в области защиты персональных данных
2	Правовые режимы доступа к информации. Безопасность в цифровой экономике	Информационная составляющая экономической безопасности в условиях цифровой экономики Программа «Цифровая экономика в РФ». Понятие цифровой экономики. Цели цифровой экономики. Условия реализации программы «Цифровая экономика в РФ». Направления развития цифровой экономики. Информационная безопасность цифровой экономики
3	Безопасность и регулирование электронного документооборота и массового распространения информации	Правовые основы электронного документооборота Документированная и недокументированная информация. Понятие и виды документов. Носители документированной информации. Документы на бумажных носителях. Понятие электронного документа. Электронная подпись и ее виды. Принципы и условия использования электронной подписи. Организации документооборота в органах государственной власти и местного самоуправления. Правила делопроизводства и документооборота. Права на материальные носители, содержащие документированную информацию. Порядок хранения и использования документированной информации в составе архивов.
3	Безопасность и регулирование электронного документооборота и массового	Правовое регулирование в сфере массовой информации Общая характеристика правового режима массовой информации. Понятие и виды средств массовой информации. Свобода массовой информации. Цензура массовой информации. Понятие злоупотребления свободой массовой информации.

	распространения информации	Субъекты правоотношений в массовой информации. Особенности правового статуса информационного агентства. Правовой статус учредителя средства массовой информации. Правовой статус главного редактора. Правовой статус журналиста. Правовой статус зарубежного корреспондента. Аккредитация журналиста
4	Информационная безопасность РФ на национальном уровне	Обеспечение национальных интересов РФ в области информационной безопасности Информационная безопасность как социальное явление. Соотношение информационной безопасности с другими видами безопасности. Безопасность информации. Защита информации и виды средств защиты информации. Информационное оружие. Информационная война. Понятие информационной безопасности детей. Государственный надзор в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию. Понятие информационной безопасности РФ. Национальные интересы РФ в информационной сфере и их обеспечение. Угрозы информационной безопасности РФ и их источники. Правовые методы обеспечения информационной безопасности РФ. Система обеспечения информационной безопасности РФ. Международное сотрудничество в области обеспечения информационной безопасности.
4	Информационная безопасность РФ на национальном уровне	Ответственность за правонарушения в информационной сфере Понятие и виды ответственности за правонарушения в информационной сфере. Уголовная ответственность за преступления в информационной сфере. Административно-правовая ответственность за правонарушения в информационной сфере. Гражданско-правовая ответственность за правонарушения в информационной сфере.
6	Информация и бизнес. Информационная безопасность	Информационная сущность бизнеса Особенности управления. Информационная сущность бизнеса. Требования к информации. Качество информации и эффективность управления. Определение информационной безопасности. Связь материальных и информационных процессов. Структура информационных потоков компании. Локальная нормативная база компании по информационной безопасности
6	Информация и бизнес. Информационная безопасность	Риски информационной безопасности Риски информационной безопасности в структуре рисков бизнеса. Возрастающая сложность информационных систем и технологий
7	Управление информационной безопасностью бизнеса	Модель обеспечения информационной безопасности организации Понятия риска, угрозы, ущерба и уязвимости. Распределение ресурсов организации в условиях риска. Риск-ориентированный подход к обеспечению информационной безопасности. Идентификация рисков. Зависимость качества оценки рисков и идентификации событий информационной безопасности от степени документированности информационных процессов компании. Накопление знаний по рискам. Модель Деминга-Шухарта. Модель обеспечения информационной безопасности бизнеса. Требования к модели информационной безопасности
7	Управление информационной безопасностью	Архитектура управления информационной безопасностью предприятия Модели непрерывного совершенствования и процессного подхода.

	бизнеса	Гибкие модели менеджмента и международные стандарты. Этапы создания системы менеджмента информационной безопасности предприятия (СМИБ). Определение области действия СМИБ. Определение политики управления информационной безопасностью. Определение методов оценки риска информационной безопасности. Инвентаризация (идентификация) рисков. Идентификация активов информационной безопасности. Оценка и классификация рисков. Подходы к оценке рисков. Выбор средств противодействия рискам информационной безопасности. Определение целей и средств контроля за рисками. Понятия контроля и защитной меры. Оценка остаточных рисков и согласование с руководством
8	Обзор основных средств обеспечения информационной безопасности	Технические средства защиты сетевой инфраструктуры Характеристика угроз непосредственного доступа в операционную среду. Характеристика угроз, реализуемых с использованием протоколов межсетевого взаимодействия. Сетевые угрозы, уязвимости и атаки, связанные с эксплуатацией межсетевых экранов. Влияние угроз на бизнес. Примеры
8	Обзор основных средств обеспечения информационной безопасности	Антивирусное программное обеспечение Угрозы. Возможности и функции современного антивирусного программного обеспечения. Влияние угроз на бизнес. Примеры
9	Документальное обеспечение информационной безопасности	Политика информационной безопасности Содержание документа "Политика информационной безопасности" и взаимосвязанных документов
11	Криптография как основа защиты данных при хранении и передаче по каналам связи	Возможности современных криптографических систем в обеспечении безопасности данных Системы шифрования. Основы блокчейн-технологии и ее использование для обеспечения целостности и доступности данных. Функции современных криптографических систем. Безопасность электронного документооборота
12	Системы защиты данных от утечек	Назначение и функции систем защиты данных от утечек (DLP-систем) Примеры, причины и последствия утечки конфиденциальных данных организации. Функции DLP-систем. Обзор рынка DLP-систем в РФ. Критерии выбора DLP-системы. Состав затрат на внедрение и эксплуатацию DLP-системы. Источники экономического эффекта от внедрения DLP-системы
13	Стандарты информационной безопасности	Требования международных и российских стандартов информационной безопасности Стандарты Банка России. PCI DSS. Особенности оценки системы информационной безопасности организации. Модель угроз. Модель нарушителя
14	Работа с инцидентами информационной безопасности. Платформа реагирования на инциденты (IRP). Security Operational Center (SOC)	Реагирование на инциденты информационной безопасности Особенности рисков информационной безопасности. Модель управления рисками информационной безопасности. Incident Responce Platform. Security Operational Center

5.2. Практические занятия

№ разд	Наименование раздела и темы практических занятий	Наименование и содержание практических занятий
1	Информация. Информационное право.	Информация как правовая категория Виды информации (обсуждение, опрос). Основы теории информации. Основные подходы к определению понятия «информация».
1	Информация. Информационное право.	Предмет, методы и система информационного права Определение понятия «информационное право». Предмет и методы информационного права. Проблематика отграничения информационного права от смежных отраслей права. Основные подходы к определению принципов информационного права
1	Информация. Информационное право.	Информационные правоотношения Понятие, признаки и виды информационных правоотношений. Основные подходы к определению объектов информационных правоотношений. Субъекты и содержание информационных правоотношений
2	Правовые режимы доступа к информации. Безопасность в цифровой экономике	Правовые режимы доступа к информации Основные информационные права и свободы, основания их ограничения. Право на доступ к информации. Понятие и виды правовых режимов свободного доступа к информации. Информация, к которой не может быть ограничен доступ. Массовая информация. Исключительные права. Общественное достояние. Понятие и виды правовых режимов ограниченного доступа к информации. Содержание конституционного права на неприкосновенность частной жизни, личную и семейную тайну. Тайна и ее разновидности. Государственная тайна: понятие и особенности правового режима. Коммерческая тайна: понятие и особенности правового режима. Служебная тайна: понятие и виды. Особенности правового режима носителей информации, составляющей тайну. Правовой режим персональных данных
3	Безопасность и регулирование электронного документооборота и массового распространения информации	Безопасность документированной информации Документированная и недокументированная информация. Понятие и виды документов. Носители документированной информации. Документы на бумажных носителях. Понятие электронного документа. Электронная подпись и ее виды. Принципы и условия использования электронной подписи.
3	Безопасность и регулирование электронного документооборота и массового распространения информации	Регулирование информации, находящейся в открытом доступе Общая характеристика и перспективы развития правового регулирования в сфере использования информационно-телекоммуникационных сетей. Понятия «сайт» и «страница сайта» в сети «Интернет». Понятие и виды доменных имен. Правовой режим информации, размещаемой в сети «Интернет». Правовой статус владельца сайта в сети «Интернет». Правовой статус провайдера хостинга. Условия ограничения доступа к сайтам в сети «Интернет». Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в РФ запрещено
4	Информационная	Правовые основы цифровой экономики в РФ

	безопасность РФ на национальном уровне	Программа «Цифровая экономика в РФ». Понятие цифровой экономики. Цели цифровой экономики. Условия реализации программы «Цифровая экономика в РФ». Направления развития цифровой экономики
4	Информационная безопасность РФ на национальном уровне	Ответственность за правонарушения в информационной сфере Понятие и виды ответственности за правонарушения в информационной сфере. Уголовная ответственность за преступления в информационной сфере. Административно-правовая ответственность за правонарушения в информационной сфере. Гражданско-правовая ответственность за правонарушения в информационной сфере
6	Информация и бизнес. Информационная безопасность	Информация как необходимое условие существования организации Управление информационными потоками организации как основа экономической безопасности. Качество информации и эффективность управления: положительные и отрицательные примеры
6	Информация и бизнес. Информационная безопасность	Риски информационной безопасности Анализ и оценка рисков информационной безопасности: примеры, задания
6	Информация и бизнес. Информационная безопасность	Взаимосвязь рисков информационной безопасности с финансовыми рисками и рисками кадровой безопасности Использование инструментов информационной безопасности для выявления финансовых рисков и рисков кадровой безопасности
7	Управление информационной безопасностью бизнеса	Управление информационной безопасностью организации Организационная структура информационной безопасности. Распределение полномочий и обязанностей между подразделениями организации по обеспечению информационной безопасности. Место информационной безопасности в структуре подразделений, отвечающих за комплексную безопасность организации. Управление рисками информационной безопасности
8	Обзор основных средств обеспечения информационной безопасности	Организация и средства защиты сети предприятия Виды и особенности технических средств защиты сети: примеры, кейсы. Обсуждение, тесты
8	Обзор основных средств обеспечения информационной безопасности	Задачи безопасности информационных активов, решаемые с помощью антивирусного программного обеспечения Функции, общая характеристика, производители антивирусного программного обеспечения. Рынок РФ. Критерии выбора специализированного программного обеспечения
9	Документальное обеспечение информационной безопасности	Локальная нормативно-правовая база по информационной безопасности организации Содержание и структура "Политики информационной безопасности". Обсуждение примера. Задания в группах. Защита заданий
11	Криптография как основа защиты данных при хранении и передаче по каналам связи	Системы безопасности электронного документооборота Возможности криптографических систем. Использование криптографии для защиты данных при передаче по каналам связи и при хранении. Индивидуальные задания на получение умений и отработку навыков использования криптографических средств защиты
11	Криптография как основа защиты	Криптография как одна из ключевых технологий блокчейн Технология блокчейн - принципы и механизмы работы. Возможности

	данных при хранении и передаче по каналам связи	использования для защиты данных
12	Системы защиты данных от утечек	Использование систем защиты данных от утечек для снижения рисков информационной и экономической безопасности Освоение работы с DLP-системой: функции, параметры, отчеты. Выполнение заданий
12	Системы защиты данных от утечек	Решение задач экономической безопасности с использованием систем мониторинга информационных потоков и противодействия утечкам данных Виды и особенности систем противодействия утечкам данных. Задачи учета использования рабочего времени и контроль соответствующих рисков кадровой безопасности; продуктивность использования рабочего времени сотрудниками; решение кейсов мошенничества, нецелевого использования сотрудниками ресурсов организации, др.
13	Стандарты информационной безопасности	Ключевые требования стандартов информационной безопасности Банка России Система документов Банка России по информационной безопасности. Содержание и структура. Основные требования
13	Стандарты информационной безопасности	Международные стандарты и сотрудничество в области информационной безопасности PCI DSS. Международные организации в области информационной безопасности. Участие и сотрудничество российских государственных и коммерческих структур
14	Работа с инцидентами информационной безопасности. Платформа реагирования на инциденты (IRP). Security Operational Center (SOC)	Система реагирования на инциденты информационной безопасности Организационная и техническая составляющая систем мониторинга и реагирования на инциденты
14	Работа с инцидентами информационной безопасности. Платформа реагирования на инциденты (IRP). Security Operational Center (SOC)	Аутсорсинг услуг информационной безопасности Состав затрат на собственную систему информационной безопасности, преимущества и недостатки. Состав затрат на аутсорсинга информационной безопасности. Преимущества и недостатки

5.3. Самостоятельная работа обучающихся

№ разд	Наименование раздела дисциплины и темы	Содержание самостоятельной работы
1	Информация. Информационное право.	Информационные правоотношения Подготовка к практическому занятию по теме. Подготовка доклада
2	Правовые режимы доступа к информации. Безопасность в цифровой экономике	Программа "Цифровая экономика РФ" Проекты программы "Цифровая экономика". Содержание программы информационной безопасности цифровой экономики. Подготовка к практическим занятиям. подготовка докладов

2	Правовые режимы доступа к информации. Безопасность в цифровой экономике	Правовые основы защиты конфиденциальных данных Правовые основы защиты конфиденциальных данных. Подготовка к практическим занятиям, подготовка докладов
3	Безопасность и регулирование электронного документооборота и массового распространения информации	Правовые основы электронного документооборота Электронная подпись. Алгоритмы шифрования, особенности, практика использования криптографических систем
3	Безопасность и регулирование электронного документооборота и массового распространения информации	Правовое регулирование в сфере массовой информации Сбор информации из открытых источников. Способы сбора, правовые основы использования информации
4	Информационная безопасность РФ на национальном уровне	Актуальные нормативные документы в области кибербезопасности Концепция национальной безопасности. Структура рисков. Риски информационной безопасности на национальном уровне. Тенденции, способы противодействия
4	Информационная безопасность РФ на национальном уровне	Ответственность за нарушения в области защиты конфиденциальных данных Ответственность за разглашение данных, составляющих государственную тайну, коммерческую тайну. Ответственность за нарушение закона о персональных данных
6	Информация и бизнес. Информационная безопасность	Управление рисками информационной безопасности Подготовка к практическим занятиям по теме. Выполнение заданий, подготовка к тестированию
6	Информация и бизнес. Информационная безопасность	Риски, связанные с информационными активами организации Подготовка к практическим занятиям, подготовка к тестированию
7	Управление информационной безопасностью бизнеса	Распределение обязанностей по обеспечению информационной безопасности организации Подготовка к практическим занятиям, подготовка докладов, подготовка к тестированию
8	Обзор основных средств обеспечения информационной безопасности	Антивирусное программное обеспечение: функции, примеры использования Подготовка к практическим занятиям, подготовка докладов
9	Документальное обеспечение информационной безопасности	Политика информационной безопасности Подготовка к практическим занятиям, подготовка докладов
9	Документальное обеспечение информационной безопасности	Организация обучения сотрудников в области информационной безопасности Подготовка к практическим занятиям и выполнение заданий
11	Криптография как основа защиты данных при хранении и передаче по каналам	Блокчейн Подготовка к практическим занятиям, подготовка докладов

	связи	
11	Криптография как основа защиты данных при хранении и передаче по каналам связи	Системы электронного документооборота Изучение возможностей систем электронного документооборота по документации производителей. Подготовка к практическим занятиям
11	Криптография как основа защиты данных при хранении и передаче по каналам связи	История развития криптографических систем подготовка к практическим занятиям, подготовка докладов
12	Системы защиты данных от утечек	Системы противодействия утечкам данных Подготовка к практическим занятиям, выполнение заданий, подготовка к тестированию
13	Стандарты информационной безопасности	Стандарты информационной безопасности Содержание стандартов информационной безопасности. Подготовка к практическим занятиям и тестированию
14	Работа с инцидентами информационной безопасности. Платформа реагирования на инциденты (IRP). Security Operational Center (SOC)	Управление инцидентами информационной безопасности Выполнение заданий, подготовка к практическим занятиям и тестированию

6. Методические материалы для самостоятельной работы обучающихся по дисциплине (модулю)

Самостоятельную работу необходимо выполнять по всем разделам программы дисциплины в форме:

- изучения рекомендуемой основной и дополнительной литературы;
- самостоятельных занятий по подбору и анализу литературных источников;
- выполнению полученных на практических занятиях заданий, включая задания проектной работы;
- поиска источников, сбора и анализа данных, расчетов, написания текста курсовой работы.

Изучение курса осуществляется в форме участия в лекционных и практических занятиях, подготовки и написания курсовой работы, самостоятельной подготовки.

На аудиторных занятиях обучающиеся знакомятся с теоретико-методологическими основами дисциплины, современными проблемами, понятиями. Освоение основных понятий требуется на уровне возможности их применения в дискуссиях на практических занятиях, при подготовке курсовой работы, выполнении проектных заданий и подготовке к круглому столу.

Проработка изучаемого материала проводится на практических занятиях, в ходе которых обучающиеся подробно анализируют основные компоненты изучаемой темы. В форме доклада или диалога с преподавателем рассматривают наиболее сложные и глубокие закономерности и механизмы, обсуждают последние публикации по изучаемым проблемам.

В течение семестра обучающиеся получают практические навыки использования системы мониторинга работы сотрудников.

Итогом изучения курса является успешная сдача зачета и экзамена.

7. Оценочные материалы для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине (модулю)

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины

№ п/п	Контролируемые разделы дисциплины (модуля)	Код и наименование индикатора контролируемой компетенции	Вид оценочного средства
1	Информация. Информационное право.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4, ПК-3.5	Устный опрос, тесты, доклады
2	Правовые режимы доступа к информации. Безопасность в цифровой экономике	ПК-3.3, ПК-3.4, ПК-3.5	Устный опрос, тесты, доклады
3	Безопасность и регулирование электронного документооборота и массового распространения информации	ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4, ПК-3.5	Устный опрос, тесты, доклады
4	Информационная безопасность РФ на национальном уровне	ПК-3.3, ПК-3.4, ПК-3.5	Устный опрос, тесты, доклады
5	Зачёт	ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4, ПК-3.5	Вопросы промежуточной аттестации
6	Информация и бизнес. Информационная безопасность	ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4, ПК-3.5	Устный опрос, тесты, задания, доклады
7	Управление информационной безопасностью бизнеса	ПК-3.3, ПК-3.5	Устный опрос, тесты, задания, доклады
8	Обзор основных средств обеспечения информационной безопасности	ПК-3.3, ПК-3.5	Устный опрос, тесты, задания, доклады
9	Документальное обеспечение информационной безопасности	ПК-3.3, ПК-3.5	Устный опрос, тесты, задания, доклады
10	Зачёт	ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4, ПК-3.5	Вопросы промежуточной

			аттестации
11	Криптография как основа защиты данных при хранении и передаче по каналам связи	ПК-3.3	Устный опрос, тесты, задания
12	Системы защиты данных от утечек	ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4, ПК-3.5	Устный опрос, тесты, задания
13	Стандарты информационной безопасности	ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4, ПК-3.5	Устный опрос, тесты
14	Работа с инцидентами информационной безопасности. Платформа реагирования на инциденты (IRP). Security Operational Center (SOC)	ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4, ПК-3.5	Устный опрос, тесты, задания
15	Иная контактная работа	ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4, ПК-3.5	Курсовая работа. Устная защита
16	Экзамен	ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4, ПК-3.5	Вопросы промежуточной аттестации (устный опрос)

7.2. Типовые контрольные задания или иные материалы текущего контроля успеваемости, необходимые для оценки знаний, умений и навыков и (или) опыта профессиональной деятельности, характеризующих этапы формирования компетенций в процессе освоения дисциплины

Групповые творческие задания (проекты) для проверки сформированности индикаторов достижения компетенций ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4, ПК-3.5.

Оцениваются знания, умения, навыки по разделам курса 1-6.

1. Разработка политики информационной безопасности.
2. Идентификация и учет информационных активов.
3. Генерация «карты» процессов обработки персональных данных (ПДн).
4. Идентификация информационных систем персональных данных (ИСПДн).
5. Разработка организационных мер по защите персональных данных.
6. Разработка программы повышения осведомлённости сотрудников в области защиты персональных данных.

Круглый стол

(перечень дискуссионных тем круглого стола для проверки сформированности индикаторов достижения компетенций ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4, ПК-3.5)

Оцениваются знания, умения, навыки по разделу 1.

Раздел 1:

1. Сравнение международных и национального законов в области защиты персональных данных.

Групповое (индивидуальное по выбору студента) творческое задание для проверки сформированности индикаторов достижения компетенций ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4, ПК-3.5.

Оцениваются знания, умения, навыки по разделам курса 1-6.

Вариант 1

Вы руководитель предприятия. Вам необходимо организовать процесс формирования «Перечня сведений конфиденциального характера». Сделайте описание бизнес-процесса.

Вариант 2

Вы руководитель предприятия. Вам необходимо организовать конфиденциальное делопроизводство. Сделайте описание бизнес-процесса.

Вариант 3

Вы руководитель предприятия. Вам необходимо организовать защиту в отношении документопотоков. Сделайте описание бизнес-процесса.

Вариант 4

Вы руководитель предприятия. Вам необходимо организовать технологическую систему обработки конфиденциальных документов. Сделайте описание бизнес-процесса.

Тестовые задания

(примеры тестовых заданий для проверки сформированности индикаторов достижения компетенций ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4, ПК-3.5)

Оцениваются знания по разделам курса 1-6.

1. Безопасность информации (в соответствии с Руководящим документом "Защита от несанкционированного доступа к информации Термины и определения") — это:

a) состояние защищенности информации, обрабатываемой средствами вычислитель-ной техники или автоматизированной системы, от внутренних или внешних угроз;

b) система управления защитой информации;

c) последовательность действий по защите от угроз?

2. Какой документ является базовым в системе локальной документации компании по информационной безопасности:

a) политика информационной безопасности;

b) правила разделения доступа;

c) регламент мониторинга инцидентов безопасности?

3. К какому типу рисков относятся риски информационной безопасности по классификации Базельского комитета по банковскому надзору:

a) стратегический;

a) операционный;

b) ликвидности;

c) рыночный?

4. Какое из перечисленных действий является первым этапом разработки системы информационной безопасности предприятия:

a) выбор средств защиты;

b) идентификация событий информационной безопасности;

c) мониторинг событий информационной безопасности?

5. DLP системы предназначены для:

a) выявления и предотвращения утечек данных;

b) выявления и предотвращения заражения вирусами;

c) выявления и предотвращения сетевых атак?

6. Двухфакторная аутентификация подразумевает использование двух из следующих способов идентификации пользователя (укажите неправильный ответ):

a) OTP;

b) пароль;

c) смарт-карта;

d) ПИН;

e) отпечаток пальца;

f) контроль документа, удостоверяющего личность.

7. Совокупность правил, определяющих разрешения и запреты доступа к информационным ресурсам — это:

a) уровень полномочий субъекта доступа;

b) правила разделения доступа;

c) модель защиты информационных ресурсов?

8. Возможность возникновения ущерба в результате нарушения информационной безопасности — это:

a) уязвимость;

b) атака;

c) риск?

9. Какое свойство защищенной информации было нарушено, если вы видите приблизительно следующий текст ошибки «сервис временно не работает, обратитесь . . .»:

a) целостность;

b) доступность;

c) конфиденциальность;

d) авторство документа?

10. Целью федерального закона о персональных данных является:

- обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну;
- обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных.

11. Персональными данными, согласно закону о персональных данных, являются:

- любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных), за исключением информации открытого доступа (общедоступные информационные ресурсы).

12. Трансграничная передача персональных данных — это:

- передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;
- передача персональных данных на территорию иностранного государства органу власти иностранного государства или иностранному юридическому лицу;
- передача персональных данных на территорию иностранного государства органу власти иностранного государства.

13. Доступность данных — это:

- состояние данных, при котором они могут быть беспрепятственно использованы любым сотрудником организации;
- состояние данных, при котором они могут быть беспрепятственно использованы любым сотрудником организации, имеющим соответствующее право доступа;
- отсутствие ошибок в данных.

14. Уязвимость информационной системы или программного продукта — это:

- слабое место;
- начавшая реализовываться атака;
- характеристика уровня безопасности информационной системы.

15. Наличие процесса управления уязвимостями, включая управление жизненным циклом программного обеспечения, patch management, pentesting является:

- необходимым, но недостаточным условием обеспечения безопасности персональных данных;
- необходимым и достаточным условием обеспечения безопасности персональных данных;
- не является необходимым и достаточным условием обеспечения безопасности персональных данных.

16. Неизменность информации в процессе ее передачи или хранения — это:

- целостность;
- конфиденциальность;

- аутентичность.

17. Федеральный закон «О персональных данных» принят:
- 27 июля 2006 года;
- 27 июня 2003 года;
- 19 мая 2010 года.

Проект «Построение концепции информационной безопасности предприятия»
(для проверки сформированности индикаторов достижения компетенций ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4, ПК-3.5)

Оцениваются знания, умения по разделам курса 3-6.

1. Цель работы

Знакомство с основными принципами построения концепции ИБ предприятия, с учетом особенностей его информационной инфраструктуры.

2. Краткие теоретические сведения

До начала создания систем информационной безопасности ряд отечественных нормативных документов (ГОСТ Р ИСО/МЭК 15408 ГОСТ Р ИСО/МЭК 27000 ГОСТ Р ИСО/МЭК 17799) и международных стандартов (ISO 27001/17799) прямо требуют разработки основополагающих документов – Концепции и Политики информационной безопасности. Если Концепция ИБ в общих чертах определяет, ЧТО необходимо сделать для защиты информации, то Политика детализирует положения Концепции, и говорит КАК, какими средствами и способами они должны быть реализованы.

Концепция информационной безопасности используется для:

• принятия обоснованных управленческих решений по разработке мер защиты информации;

• выработки комплекса организационно-технических и технологических мероприятий по выявлению угроз информационной безопасности и предотвращению последствий их реализации;

• координации деятельности подразделений по созданию, развитию и эксплуатации информационной системы с соблюдением требований обеспечения безопасности информации;

• и, наконец, для формирования и реализации единой политики в области обеспечения информационной безопасности.

3. Задание

Разработать концепцию информационной безопасности компании, содержащую следующие основные разделы (приведен примерный план, в который в случае необходимости могут быть внесены изменения).

1. Общие положения

Назначение Концепции по обеспечению информационной безопасности.

1.2. Цели системы информационной безопасности

1.3. Задачи системы информационной безопасности.

2. Проблемная ситуация в сфере информационной безопасности

2.1. Объекты информационной безопасности.

2.2. Определение вероятного нарушителя.

2.3. Описание особенностей (профиля) каждой из групп вероятных нарушителей.

2.4. Основные виды угроз информационной безопасности Предприятия.

• Классификации угроз.

• Основные непреднамеренные искусственные угрозы.

• Основные преднамеренные искусственные угрозы.

2.5. Общестатистическая информация по искусственным нарушениям информационной безопасности.

2.6. Оценка потенциального ущерба от реализации угрозы (см. Практическую работу № 1).

3. Механизмы обеспечения информационной безопасности Предприятия

3.1. Принципы, условия и требования к организации и функционированию системы информационной безопасности.

3.2. Основные направления политики в сфере информационной безопасности.

3.3. Планирование мероприятий по обеспечению информационной безопасности

Предприятия.

3.4. Критерии и показатели информационной безопасности Предприятия.

4. Мероприятия по реализации мер информационной безопасности Предприятия

4.1. Организационное обеспечение информационной безопасности.

• Задачи организационного обеспечения информационной безопасности.

• Подразделения, занятые в обеспечении информационной безопасности.

• Взаимодействие подразделений, занятых в обеспечении информационной безопасности.

4.2. Техническое обеспечение информационной безопасности Предприятия.

• Общие положения.

• Защита информационных ресурсов от несанкционированного доступа.

• Средства комплексной защиты от потенциальных угроз.

• Обеспечение качества в системе безопасности.

• Принципы организации работ обслуживающего персонала.

4.3. Правовое обеспечение информационной безопасности Предприятия.

• Правовое обеспечение юридических отношений с работниками Предприятия .

• Правовое обеспечение юридических отношений с партнерами Предприятия.

• Правовое обеспечение применения электронной цифровой подписи.

4.4. Оценивание эффективности системы информационной безопасности Предприятия.

5. Программа создания системы информационной безопасности Предприятия

StaffCop

(задание для проверки сформированности навыков по индикатору достижения компетенции ПК-3.4)

2.1. Изменение расписания. Отчеты по учету рабочего времени.

2.1.1. Сделать отчет "Комбинированный отчет", меню "Учет рабочего времени.

2.1.2. Сделать развернутый отчет по одному из пользователей (левая кнопка мыши на имени компьютера).

Зафиксировать продуктивность или непродуктивность работы в каком-либо приложении или на сайте.

2.1.3. Изменить категорию продуктивности приложения или сайта (Фильтры - Политики - Политики продуктивности - категории приложений или категории веб-ресурсов).

2.1.4. Проявить активность в приложении / веб-ресурсе, по которому была изменена категория продуктивности (новая категория продуктивности применяется только для новых событий).

2.1.5. Сделать отчет "Комбинированный отчет", меню "Учет рабочего времени, убедившись в изменении категоризации активности с продуктивной на непродуктивную или наоборот.

2.1.6. Создать рабочее расписание (Админ - Рабочее расписание).

2.1.7. Назначить созданное рабочее расписание компьютеру, за которым Вы работаете (Админ - Назначение расписания).

2.1.8. Сделать отчет "Комбинированный отчет", меню "Учет рабочего времени, убедившись в изменении параметров расписания.

В отчет:

- отчет до изменения категории продуктивности и расписания;
- отчет после изменения категории продуктивности;
- отчет после изменения расписания.

Темы докладов

(для проверки сформированности индикаторов достижения компетенций ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4, ПК-3.5)

Оцениваются знания, умения по разделам курса 1-4.

1. Информация как правовая категория: понятие и основные критерии классификации.

2. Правовые режимы информации: понятие и виды.

3. Правовые режимы ограниченного доступа к информации: понятие и общая характеристика.

4. Тайна и ее разновидности.

5. Понятие и виды конфиденциальной информации.
6. Государственная тайна.
7. Признаки сведений, составляющих государственную тайну.
8. Гриф секретности: понятие и порядок использования.
9. Правовой режим носителей сведений, составляющих государственную тайну.
10. Допуск к государственной тайне.
11. Доступ к сведениям, составляющим государственную тайну.
12. Основания и порядок отнесения сведений к государственной тайне.
13. Основания и порядок рассекречивания сведений, составляющих государственную тайну.
14. Коммерческая тайна.
15. Особенности правовой охраны конфиденциальности информации в рамках трудовых отношений.
16. Банковская тайна.
17. Служебная тайна.
18. Адвокатская тайна.
19. Аудиторская тайна.
20. Врачебная тайна.
21. Медицинская тайна.
22. Налоговая тайна.
23. Нотариальная тайна.
24. Тайна связи.
25. Тайна совещания судей.
26. Тайна совещания присяжных заседателей.
27. Тайна страхования.
28. Тайна усыновления (удочерения).
29. Правовой режим инсайдерской информации.
30. Правовой режим данных предварительного расследования.
31. Правовой режим сведений о государственной регистрации актов гражданского состояния.
32. Правовой режим сведений о защищаемом лице.
33. Признаки сведений, составляющих тайну завещания.
34. Признаки сведений, составляющих профессиональную тайну ломбардов.
35. Правовой режим сведений о сущности изобретения.
36. Особенности правового режима сведений, составляющих секретное изобретение.
37. Правовой режим сведений о сущности полезной модели.
38. Правовой режим сведений о сущности промышленного образца.
39. Особенности правового режима сведений, составляющих секрет производства (ноу-хау).
40. Особенности правового режима сведений, составляющих секрет производства (ноу-хау).
41. Особенности правового режима сведений, составляющих служебный секрет производства (ноу-хау).
42. Ответственность за нарушение законодательства Российской Федерации о государственной тайне.
43. Ответственность за нарушение законодательства Российской Федерации о коммерческой тайне.
44. Ответственность за разглашение сведений, составляющих банковскую тайну.
45. Правовой режим массовой информации.
46. Средства массовой информации: понятие и виды.
47. Особенности правового статуса информационного агентства.
48. Правовой статус учредителя средства массовой информации.
49. Правовой статус главного редактора.
50. Правовой статус журналиста.
51. Правовой статус зарубежного корреспондента.
52. Ответственность за нарушение законодательства о средствах массовой информации.

53. Правовой режим персональных данных.
54. Условия обработки персональных данных.
55. Биометрические персональные данные.
56. Права субъекта персональных данных.
57. Ответственность за нарушение законодательства Российской Федерации о персональных данных.
58. Правовой статус библиотеки.
59. Особенности правового режима библиотечных фондов.
60. Архив: понятие и виды.
61. Архивный документ: понятие и виды.
62. Правовые режимы доступа к архивным документам.
63. Особенности правового регулирования использования сети «Интернет».
64. Правовой статус владельца сайта в сети "Интернет".
65. Правовой статус провайдера хостинга.
66. Понятие информационной безопасности Российской Федерации.
67. Система обеспечения информационной безопасности Российской Федерации.
68. Государственный надзор в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию.
69. Уголовная ответственность за преступления в информационной сфере.
70. Административно-правовая ответственность за правонарушения в информационной сфере.
71. Качество управления информационными активами как существенный фактор обеспечения прибыльности бизнеса.
72. Место информационной безопасности в иерархии рисков бизнеса.
73. Влияние качества информации на результаты работы предприятия и качество его администрирования.
74. Роль высшего руководства компании в обеспечении информационной безопасности. Связь системы менеджмента информационной безопасности с системой менеджмента компании.
75. Роль мониторинга в обеспечении информационной безопасности.

Темы докладов
(для проверки сформированности индикаторов достижения компетенций ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4, ПК-3.5)
Оцениваются знания, умения по разделам курса 5, 6.
76. Процедура проведения аудита на соответствие регуляторным требованиям в области защиты персональных данных.
77. Понятие и классификация информационных систем персональных данных.
78. Инвентаризация информационных ресурсов.
79. Обзор систем защиты информационных активов.
80. Системы защиты данных от утечек.
81. Средства защиты конфиденциальных данных от несанкционированного доступа при передаче и хранении.
82. Обезличивание данных: причины и способы.
83. Выявление актуальных угроз безопасности конфиденциальных данных.
84. Методы оценки экономической целесообразности внедрения средств защиты данных.
85. Каналы утечки конфиденциальных данных: анализ современной ситуации.
86. Организация системы защиты данных на предприятии.
87. Разработка требований к системе информационной безопасности.
88. Состав затрат на разработку (приобретение) и внедрение системы защиты данных.

7.3. Система оценивания результатов обучения по дисциплине (модулю) при проведении текущего контроля успеваемости

Оценка «отлично» (зачтено)	знания: - систематизированные, глубокие и полные знания по всем разделам дисциплины, а также по основным вопросам, выходящим за пределы учебной программы; - точное использование научной терминологии, систематически грамотное и логически правильное изложение ответа на вопросы; - полное и глубокое усвоение основной и дополнительной литературы, рекомендованной рабочей программой по дисциплине (модулю) умения: - умеет ориентироваться в теориях, концепциях и направлениях дисциплины и давать им критическую оценку, используя научные достижения других дисциплин навыки: - высокий уровень сформированности заявленных в рабочей программе компетенций; - владеет навыками самостоятельно и творчески решать сложные проблемы и нестандартные ситуации; - применяет теоретические знания для выбора методики выполнения заданий; - грамотно обосновывает ход решения задач; - безупречно владеет инструментарием учебной дисциплины, умение его эффективно использовать в постановке научных и практических задач; - творческая самостоятельная работа на практических/семинарских/лабораторных занятиях, активно участвует в групповых обсуждениях, высокий уровень культуры исполнения заданий
Оценка «хорошо» (зачтено)	знания: - достаточно полные и систематизированные знания по дисциплине; - усвоение основной и дополнительной литературы, рекомендованной рабочей программой по дисциплине (модулю) умения: - умеет ориентироваться в основных теориях, концепциях и направлениях дисциплины и давать им критическую оценку; - использует научную терминологию, лингвистически и логически правильно излагает ответы на вопросы, умеет делать обоснованные выводы; - владеет инструментарием по дисциплине, умение его использовать в постановке и решении научных и профессиональных задач навыки: - самостоятельная работа на практических занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий; - средний уровень сформированности заявленных в рабочей программе компетенций; - без затруднений выбирает стандартную методику выполнения заданий; - обосновывает ход решения задач без затруднений

Оценка «удовлетворительно» (зачтено)	знания: - достаточный минимальный объем знаний по дисциплине; - усвоение основной литературы, рекомендованной рабочей программой; - использование научной терминологии, стилистическое и логическое изложение ответа на вопросы, умение делать выводы без существенных ошибок умения: - умеет ориентироваться в основных теориях, концепциях и направлениях по дисциплине и давать им оценку; - владеет инструментарием учебной дисциплины, умение его использовать в решении типовых задач; - умеет под руководством преподавателя решать стандартные задачи навыки: - работа под руководством преподавателя на практических занятиях, допустимый уровень культуры исполнения заданий; - достаточный минимальный уровень сформированности заявленных в рабочей программе компетенций; - испытывает затруднения при обосновании алгоритма выполнения заданий
Оценка «неудовлетворительно» (не зачтено)	знания: - фрагментарные знания по дисциплине; - отказ от ответа (выполнения письменной работы); - знание отдельных источников, рекомендованных рабочей программой по дисциплине; умения: - не умеет использовать научную терминологию; - наличие грубых ошибок навыки: - низкий уровень культуры исполнения заданий; - низкий уровень сформированности заявленных в рабочей программе компетенций; - отсутствие навыков самостоятельной работы; - не может обосновать алгоритм выполнения заданий

7.4. Теоретические вопросы и практические задания для проведения промежуточной аттестации обучающихся, необходимые для оценки знаний, умений и навыков и (или) опыта профессиональной деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

7.4.1. Теоретические вопросы для проведения промежуточной аттестации обучающихся

Примерный перечень вопросов по разделам 1, 2 (семестр1 изучения дисциплины)

1. Предмет и методы информационного права.
2. Принципы информационного права.
3. Система и источники информационного права.
4. Информация как правовая категория: понятие и основные критерии классификации.
5. Информационные правоотношения: понятие, признаки и виды.
6. Содержание информационных правоотношений.
7. Понятие и виды документов.
8. Нормы информационного права и их действие в пространстве и во времени.
9. Правовые режимы информации: понятие и виды.
10. Правовые режимы ограниченного доступа к информации: понятие и общая характеристика.
11. Тайна и ее разновидности.
12. Средства защиты информации.
13. Понятие и виды конфиденциальной информации.
14. Государственная тайна.
15. Признаки сведений, составляющих государственную тайну.

16. Степени секретности сведений, составляющих государственную тайну.
17. Гриф секретности: понятие и порядок использования.
18. Правовой режим носителей сведений, составляющих государственную тайну.
19. Допуск к государственной тайне.
20. Доступ к сведениям, составляющим государственную тайну.
21. Основания и порядок отнесения сведений к государственной тайне.
22. Основания и порядок рассекречивания сведений, составляющих государственную тайну.
23. Коммерческая тайна.
24. Признаки сведений, составляющих коммерческую тайну.
25. Гриф «Коммерческая тайна»: понятие и порядок использования.
26. Сведения, которые не могут составлять коммерческую тайну.
27. Понятие разглашения информации, составляющей коммерческую тайну.
28. Особенности правовой охраны конфиденциальности информации в рамках трудовых отношений.
29. Банковская тайна.
30. Признаки сведений, составляющих банковскую тайну.
31. Служебная тайна.
32. Адвокатская тайна.
33. Аудиторская тайна.
34. Врачебная тайна.
35. Медицинская тайна.
36. Налоговая тайна.
37. Нотариальная тайна.
38. Тайна связи.
39. Тайна совещания судей.
40. Тайна совещания присяжных заседателей.
41. Тайна страхования.
42. Тайна усыновления (удочерения).
43. Правовой режим инсайдерской информации.
44. Правовой режим данных предварительного расследования.
45. Правовой режим сведений о государственной регистрации актов гражданского состояния.
46. Правовой режим сведений о защищаемом лице.
47. Признаки сведений, составляющих тайну завещания.
48. Признаки сведений, составляющих профессиональную тайну ломбардов.
49. Правовой режим сведений о сущности изобретения.
50. Особенности правового режима сведений, составляющих секретное изобретение.
51. Правовой режим сведений о сущности полезной модели.
52. Правовой режим сведений о сущности промышленного образца.
53. Особенности правового режима сведений, составляющих секрет производства (ноу-хау).
54. Понятие электронного документа.
55. Электронная подпись и ее виды.
56. Ответственность за нарушение законодательства Российской Федерации о государственной тайне.
57. Ответственность за нарушение законодательства Российской Федерации о коммерческой тайне.
58. Ответственность за непредоставление органам государственной власти и органам местного самоуправления информации, составляющей коммерческую тайну.
59. Ответственность за разглашение сведений, составляющих банковскую тайну.
60. Правовой режим массовой информации.
61. Понятие массовой информации.
62. Цензура массовой информации.
63. Средства массовой информации: понятие и виды.
64. Особенности правового статуса информационного агентства.

65. Правовой статус учредителя средства массовой информации.
66. Правовой статус главного редактора.
67. Правовой статус журналиста.
68. Правовой статус зарубежного корреспондента.
69. Аккредитация журналиста.
70. Понятие злоупотребления свободой массовой информации.
71. Ответственность за нарушение законодательства о средствах массовой информации.
72. Правовой режим персональных данных.
73. Понятие обработки персональных данных.
74. Принципы обработки персональных данных.
75. Условия обработки персональных данных.
76. Биометрические персональные данные.
77. Права субъекта персональных данных.
78. Обязанности оператора при сборе персональных данных.
79. Ответственность за нарушение законодательства Российской Федерации о персональных данных.
80. Правовой статус библиотеки.
81. Особенности правового режима библиотечных фондов.
82. Архив: понятие и виды.
83. Архивный документ: понятие и виды.
84. Правовые режимы доступа к архивным документам.
85. Особенности правового регулирования использования сети «Интернет».
86. Понятие сайта в сети "Интернет".
87. Понятие страницы сайта в сети "Интернет".
88. Понятие доменного имени.
89. Правовой статус владельца сайта в сети "Интернет".
90. Правовой статус провайдера хостинга.
91. Понятие информационной безопасности Российской Федерации.
92. Национальные интересы Российской Федерации в информационной сфере.
93. Виды угроз информационной безопасности Российской Федерации.
94. Правовые методы обеспечения информационной безопасности Российской Федерации.
95. Система обеспечения информационной безопасности Российской Федерации.
96. Понятие информационной безопасности детей.
97. Государственный надзор в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию.
98. Защита информации как правовая категория.
99. Уголовная ответственность за преступления в информационной сфере.
100. Административно-правовая ответственность за правонарушения в информационной сфере.

Примерный перечень вопросов по разделам 3, 4 (семестр 2 изучения дисциплины)
1. Бизнес и информация. Информационная сущность бизнеса.
2. Риск-ориентированный подход к обеспечению информационной безопасности бизнеса.
3. Назначение и общая характеристика DLP-систем.
4. Назначение и общая характеристика SIEM-систем.
5. Назначение и общая характеристика Threat Intelligence.
6. Системы шифрования как средство обеспечения защиты от несанкционированного доступа при хранении и передаче данных.
7. Электронно-цифровая подпись. Обеспечение целостности и подтверждения авторства.
8. Алгоритм формирования и проверки электронной цифровой подписи на примере системы PGP.
9. Комплексный подход к обеспечению информационной безопасности.
10. Безопасность как специфическая совокупность условий деятельности.
11. Основные положения стандарта Банка России СТО/РС БР ИББС.

12. Основные положения стандарта PCI DSS.

13. Организация системы безопасности и субъекты обеспечения безопасности предприятия.

14. Основные виды угроз безопасности. Обстоятельства, способы и субъекты их реализации.

15. Организация мониторинга информационной безопасности.

16. Безопасность мобильных приложений.

17. Особенности обеспечения безопасности облачных сервисов.

18. Модель непрерывного совершенствования информационной безопасности.

19. Реализация процессного подхода к обеспечению информационной безопасности.

20. Характеристика системы стандартов СМИБ.

21. Этапы разработки системы менеджмента информационной безопасности.

22. Структура частных менеджментов информационной безопасности.

23. Взаимосвязь менеджмента инцидентов и мониторинга информационной безопасности.

24. Основные положения методологии ITIL.

25. Спецификация процессов комплекса документов стандарта COBIT.

26. Экономическая эффективность внедрения средств обеспечения информационной безопасности.

27. SOC. Понятие. Назначение. Общая характеристика.

28. Цикл Деминга-Шухарта в управлении информационной безопасностью.

29. Система рисков предприятия и место рисков информационной безопасности в данной системе.

30. Понятие процессов и проектов применительно к информационной безопасности.

31. Подразделения, участвующие в реализации функций информационной безопасности и их взаимодействие.

32. Организация взаимодействия подразделений информационных технологий и информационной безопасности.

33. Адаптивные технологии управления информационной безопасностью.

34. Причины мотивации сотрудников предприятия к нарушению информационной безопасности.

35. Мотивация сотрудников предприятия к активному участию в разработке и поддержанию эксплуатации мер информационной безопасности.

36. Влияние корпоративной культуры на мотивацию сотрудников в области информационной безопасности.

37. Процесс отбора претендентов на должности офицеров информационной безопасности.

38. Требования к офицерам информационной безопасности.

39. Организация обучения сотрудников компании по информационной безопасности.

40. Взаимодействие компании с регулирующими органами по информационной безопасности.

41. Проектирование SOC.

42. Мониторинг событий информационной безопасности.

43. Организация работы с инцидентами информационной безопасности.

44. Аутсорсинг информационной безопасности.

45. Расчет затрат на внедрение SOC.

46. Текущие тенденции и перспективы развития систем обеспечения информационной безопасности.

47. Профессиональные сообщества в области информационной безопасности: характеристика, функции.

48. Обзор наиболее значимых в РФ компаний, оказывающих услуги в области информационной безопасности.

49. Анализ статистики по наиболее актуальным угрозам информационной безопасности.

50. Наиболее значимые хакерские преступные группировки: характеристика деятельности, примеры инцидентов.

51. Примеры веерных атак на информационные ресурсы.

52. Примеры целевых атак на информационные ресурсы.

53. Международное сотрудничество в области информационной безопасности.

54. Особенности финансовых организаций при обеспечении информационной безопасности.
55. Особенности защиты объектов критической информационной инфраструктуры.
56. Особенности защиты государственных и муниципальных предприятий.
57. Требования к средствам криптографической защиты информации.
58. Информационная безопасность как фактор повышения операционной эффективности компании.
59. Регулирование информационной безопасности — обзор нормативно-правовой базы.
60. Место информационной безопасности в процессах цифровизации предприятий.

Примерный перечень вопросов по разделам 5, 6 (семестр 3 изучения дисциплины)
1. Функции оператора персональных данных.
2. Ответственность за нарушения в области информационной безопасности
3. Условия обработки персональных данных (согласно закону о персональных данных).
4. Состав внутренних документов компании по организации защиты конфиденциальных данных.
5. Особенности обработки персональных данных уволенных работников.
6. Особенности обработки персональных данных соискателей на замещение вакантных должностей.
7. Избыточность обработки персональных данных.
8. Назначение и характеристика модели угроз.
9. Расчет затрат на внедрение и использование системы защиты данных.
10. Направления сокращения затрат на создание системы защиты данных.
11. Особенности защиты данных от утечек.
12. Методика выбора мер по обеспечению безопасности данных.
13. Характеристика видов угроз безопасности данных.
14. Классификация средств защиты данных.
15. Обязанности оператора при обработке персональных данных.
16. Меры обеспечения безопасной обработки данных.
17. Уведомление об обработке персональных данных.
18. Права субъектов персональных данных.
19. Согласие субъекта персональных данных на обработку персональных данных.
20. Специальные категории персональных данных.
21. Характеристика биометрических персональных данных.
22. Принципы обработки конфиденциальных данных.
23. Требования к обучению сотрудников в области защиты персональных данных.
24. Цикл Деминга в организации защиты персональных данных.
25. Интеграция системы защиты персональных данных в систему информационной безопасности компании.
26. Документы ФСТЭК в области защиты персональных данных.
27. Проверки Роскомнадзора в области защиты данных.
28. Управление инцидентами информационной безопасности.
29. Банк данных угроз информационной безопасности персональных данных.
30. Политика обработки персональных данных — содержание документа.
31. Модель угроз информационной безопасности — содержание документа.
32. Методические указания Роскомнадзора по защите персональных данных (для субъектов персональных данных).
33. Конфликт требований законодательства по защите персональных данных и использования систем мониторинга работы сотрудников.
34. Положения Конституции РФ, связанные с защитой персональных данных.
35. Основные положения GDPR.
36. Способы незаконного использования персональных данных. Примеры.
37. Кибербуллинг: характеристика, примеры.
38. Источники утечек персональных данных.
39. История развития законодательной базы защиты персональных данных в РФ.
40. Зарубежное законодательство по защите персональных данных.

41. Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных.

42. Определение персональных данных: 152 ФЗ, Трудовой Кодекс, GDPR, др.

43. Документы Правительства РФ в области защиты персональных данных.

44. Обезличивание персональных данных — понятие, требования законодательства, методы обезличивания.

45. Характеристика рынка персональных данных: участники, цели приобретения персональных данных.

46. Примеры утечек персональных данных в РФ.

47. Примеры утечек персональных данных за пределами РФ.

48. Трансграничная передача персональных данных.

49. Особенности обработки персональных данных в государственных и муниципальных системах персональных данных.

50. Биометрические персональные данные.

51. Характеристика правовых (нормативных), организационных и технических мер защиты конфиденциальных данных. Примеры.

52. Уровни защищенности персональных данных.

53. Обязанности оператора по устранению нарушений законодательства, допущенных при обработке персональных данных (статья 21 главы 4 ФЗ-152).

54. Обязанности лица, ответственного за организацию обработки персональных данных.

55. Государственный контроль и надзор в области защиты персональных данных.

56. Ответственность, предусмотренная за нарушение законодательства в области защиты персональных данных.

57. Роскомнадзор — цели, задачи, функции.

58. Значение персонала компании как субъекта угроз безопасности персональных данных.

7.4.2. Практические задания для проведения промежуточной аттестации обучающихся

Примеры практических заданий

1. Разработать схему бизнес-процесса управления инцидентами информационной безопасности для предприятия. В описании задания привести характеристику предприятия: вид деятельности, масштаб, географическая распределенность подразделений, подразделения, участвующие в управлении инцидентами.

2. Продемонстрировать последовательность действий в интерфейсе StaffCop по созданию фильтра для поиска событий, связанных с определенным документом. Ограничить период времени (по датам), каналы передачи информации.

3. Создать интеллектуальную карту в сервисе Miro по теме "Управление операционными рисками".

4. Создать интеллектуальную карту в сервисе Miro по классификации угроз информационной безопасности. В описании задания привести характеристику предприятия.

5. Определить уровень защищенности и требования к защите для выбранного Вами предприятия. В описании задания привести характеристику предприятия.

7.4.3. Примерные темы курсовой работы (проекта) (при наличии)

Темы курсовой работы

1. Идентификация и аутентификация пользователей, не являющихся сотрудниками организации.

2. Управление доступом к конфиденциальным данным.

3. Нормативно-правовые основы защиты персональных данных в РФ.

4. Протокол Европейского союза по защите персональных данных.

5. Законодательство США по защите персональных данных.

6. Использование блокчейн для защиты конфиденциальных данных.

7. Управление информационной безопасностью на базе ISO/IEC 27001.

8. Меры защиты информации согласно ISO/IEC 27002.

9. Политика информационной безопасности как ключевой локальный нормативный акт по защите данных.

10. Организация защиты персональных данных на предприятии.
11. Данные как основной ресурс цифровой экономики.
12. Политика Facebook (другой социальной сети по выбору студента) в области защиты персональных данных.
13. Анализ мировой индустрии торговли персональными данными.
14. Управление инцидентами информационной безопасности.
15. Назначение и функции DLP-систем.
16. Анализ российского рынка DLP-систем.
17. Характеристика основных угроз информационной безопасности в 2020 году.
18. Способы обезличивания персональных данных.
19. Брокеры данных - Data Brokers (Acxiom, Equifax, CoreLogic, др.).
20. Характеристика действующих в РФ хакерских группировок.
21. Характеристика индустрии защиты данных в РФ.
22. Мошенничество с электронной подписью в РФ.
23. Судебная практика по преступлениям, связанным с компрометацией конфиденциальных данных.
24. Последствия реализации рисков информационной безопасности для предприятия.
25. Последствия компрометации персональных данных для гражданина.
26. Рекомендации для гражданина по защите персональных данных.
27. Цифровой профиль гражданина РФ.
28. Цифровые государственные сервисы (на примере любой страны по выбору обучающегося).
29. Единая система биометрической идентификации в РФ.
30. Локальная нормативная база предприятия в области обеспечения безопасности персональных данных (состав и структура документов).

7.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта профессиональной деятельности, характеризующие этапы формирования компетенций

Процедура проведения промежуточной аттестации и текущего контроля успеваемости регламентируется локальным нормативным актом, определяющим порядок организации и проведения текущего контроля успеваемости и промежуточной аттестации обучающихся.

Процедура оценивания формирования компетенций при проведении текущего контроля приведена в п. 7.2.

Типовые контрольные задания или иные материалы текущего контроля приведены в п. 7.3.

Промежуточная аттестация по дисциплине проводится в форме зачета (4, 5 сем.) и экзамена (6 сем.).

Зачет проводится в форме компьютерного тестирования на последнем практическом занятии семестра.

Экзамен проводится в устной форме.

7.6. Критерии оценивания сформированности компетенций при проведении промежуточной аттестации

Критерии оценивания	Уровень освоения и оценка			
	Оценка «неудовлетворительно»	Оценка «удовлетворительно»	Оценка «хорошо»	Оценка «отлично»
	«не зачтено»	«зачтено»		

	Уровень освоения компетенции «недостаточный». Компетенции не сформированы. Знания отсутствуют, умения и навыки не сформированы	Уровень освоения компетенции «пороговый». Компетенции сформированы. Сформированы базовые структуры знаний. Умения фрагментарны и носят репродуктивный характер. Демонстрируется низкий уровень самостоятельности практического навыка.	Уровень освоения компетенции «продвинутый». Компетенции сформированы. Знания обширные, системные. Умения носят репродуктивный характер, применяются к решению типовых заданий. Демонстрируется достаточный уровень самостоятельности устойчивого практического навыка.	Уровень освоения компетенции «высокий». Компетенции сформированы. Знания аргументированные, всесторонние. Умения успешно применяются к решению как типовых, так и нестандартных творческих заданий. Демонстрируется высокий уровень самостоятельности, высокая адаптивность практического навыка
знания	Обучающийся демонстрирует: -существенные пробелы в знаниях учебного материала; -допускаются принципиальные ошибки при ответе на основные вопросы билета, отсутствует знание и понимание основных понятий и категорий; -непонимание сущности дополнительных вопросов в рамках заданий билета.	Обучающийся демонстрирует: -знания теоретического материала; -неполные ответы на основные вопросы, ошибки в ответе, недостаточное понимание сущности излагаемых вопросов; -неуверенные и неточные ответы на дополнительные вопросы.	Обучающийся демонстрирует: -знание и понимание основных вопросов контролируемого объема программного материала; - знания теоретического материала -способность устанавливать и объяснять связь практики и теории, выявлять противоречия, проблемы и тенденции развития; -правильные и конкретные, без грубых ошибок, ответы на поставленные вопросы.	Обучающийся демонстрирует: -глубокие, всесторонние и аргументированные знания программного материала; -полное понимание сущности и взаимосвязи рассматриваемых процессов и явлений, точное знание основных понятий, в рамках обсуждаемых заданий; -способность устанавливать и объяснять связь практики и теории, -логически последовательные, содержательные, конкретные и исчерпывающие ответы на все задания билета, а также дополнительные вопросы экзаменатора.

умения	При выполнении практического задания билета обучающийся продемонстрировал недостаточный уровень умений. Практические задания не выполнены Обучающийся не отвечает на вопросы билета при дополнительных наводящих вопросах преподавателя.	Обучающийся выполнил практическое задание билета с существенными неточностями. Допускаются ошибки в содержании ответа и решении практических заданий. При ответах на дополнительные вопросы было допущено много неточностей.	Обучающийся выполнил практическое задание билета с небольшими неточностями. Показал хорошие умения в рамках освоенного учебного материала. Предложенные практические задания решены с небольшими неточностями. Ответил на большинство дополнительных вопросов.	Обучающийся правильно выполнил практическое задание билета. Показал отличные умения в рамках освоенного учебного материала. Решает предложенные практические задания без ошибок Ответил на все дополнительные вопросы.
владение навыками	Не может выбрать методику выполнения заданий. Допускает грубые ошибки при выполнении заданий, нарушающие логику решения задач. Делает некорректные выводы. Не может обосновать алгоритм выполнения заданий.	Испытывает затруднения по выбору методики выполнения заданий. Допускает ошибки при выполнении заданий, нарушения логики решения задач. Испытывает затруднения с формулированием корректных выводов. Испытывает затруднения при обосновании алгоритма выполнения заданий.	Без затруднений выбирает стандартную методику выполнения заданий. Допускает ошибки при выполнении заданий, не нарушающие логику решения задач Делает корректные выводы по результатам решения задачи. Обосновывает ход решения задач без затруднений.	Применяет теоретические знания для выбора методики выполнения заданий. Не допускает ошибок при выполнении заданий. Самостоятельно анализирует результаты выполнения заданий. Грамотно обосновывает ход решения задач.

Оценка по дисциплине зависит от уровня сформированности компетенций, закрепленных за дисциплиной, и представляет собой среднее арифметическое от выставленных оценок по отдельным результатам обучения (знания, умения, владение навыками).

Оценка «отлично»/«зачтено» выставляется, если среднее арифметическое находится в интервале от 4,5 до 5,0.

Оценка «хорошо»/«зачтено» выставляется, если среднее арифметическое находится в интервале от 3,5 до 4,4.

Оценка «удовлетворительно»/«зачтено» выставляется, если среднее арифметическое находится в интервале от 2,5 до 3,4.

Оценка «неудовлетворительно»/«не зачтено» выставляется, если среднее арифметическое находится в интервале от 0 до 2,4.

8. Учебно-методическое и материально-техническое обеспечение дисциплины (модуля)

8.1. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины (модуля)

№ п/п	Автор, название, место издания, издательство, год издания учебной и учебно-методической литературы	Количество экземпляров/электронный адрес ЭБС
	Основная литература	
1	Сафонова Л. А., Экономические аспекты информационной безопасности, Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2019	http://www.iprbookshop.ru/90606.html
2	Федотов М. А., Антонова А. В., Будник Р. А., Войниканис Е. А., Околеснова О. А., Петрин И. В., Примакова А. В., Семенова Е. В., Тедеев А. А., Шаблинский И. Г., Информационное право, Москва: Юрайт, 2020	https://urait.ru/bcode/451031
3	Запечников С. В., Казарин О. В., Тарасов А. А., Криптографические методы защиты информации, Москва: Юрайт, 2020	https://urait.ru/bcode/450538
4	Сычев Ю. Н., Стандарты информационной безопасности. Защита и обработка конфиденциальных документов, Саратов: Вузовское образование, 2018	http://www.iprbookshop.ru/72345.html
5	Нестеров С. А., Основы информационной безопасности, Санкт-Петербург: Лань, 2021	https://e.lanbook.com/book/165837
	Дополнительная литература	
1	Рассолов И. М., Информационное право, Москва: Юрайт, 2022	https://urait.ru/bcode/488767
2	Волков Ю. В., Информационное право. Информация как правовая категория, Москва: Юрайт, 2020	https://urait.ru/bcode/455553
3	Ковалева Н. Н., Жирнова Н. А., Тугушева Ю. М., Холодная Е. В., Информационное право. Практикум, Москва: Юрайт, 2020	https://urait.ru/bcode/449378
4	Анисимов А. А., Менеджмент в сфере информационной безопасности, Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020	http://www.iprbookshop.ru/89443.html
5	Боташева Л. Э., Трофимов М. С., Информационное право, Ставрополь: Северо-Кавказский федеральный университет, 2014	http://www.iprbookshop.ru/62840.html
6	Корабельников С. М., Преступления в сфере информационной безопасности, Москва: Юрайт, 2020	https://urait.ru/bcode/448295

Обучающиеся из числа инвалидов и лиц с ОВЗ обеспечиваются печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

8.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Наименование ресурса сети «Интернет»	Электронный адрес ресурса
Информационно-справочная система «Консультант Плюс» (дата обращения - 07.07.21)	http://www.consultant.ru/
Информационно-справочная система «Гарант» (дата обращения - 07.07.21)	http://www.garant.ru/
Российская газета (дата обращения - 07.07.21)	http://www.rg.ru

Информационная безопасность: рынок России	https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_(%D1%80%D1%8B%D0%BD%D0%BE%D0%BA_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8)
Курс "Основы информационной безопасности"	https://intuit.ru/studies/courses/10/10/info
Официальный сайт компании "Атом-безопасность"	https://www.staffcop.ru/

8.3. Перечень современных профессиональных баз данных и информационных справочных систем

Наименование	Электронный адрес ресурса
Образовательные интернет-ресурсы СПбГАСУ	https://www.spbgasu.ru/Universitet/Biblioteka/Obrazovatelnye_internet-resursy/
Журналы издательства Sage. В настоящее время доступны статьи из 320 журналов по 36 предметным рубрикам: гуманитарные и общественные науки, информатика, инженерные дисциплины, экономика, здоровье и образование.	www.sagepublications.com
Библиотека по Естественным наукам Российской Академии наук (РАН)	www.ras.ru
Аналитический портал по экономическим дисциплинам	www.economicus.ru
Единый электронный ресурс учебно-методической литературы СПбГАСУ	www.spbgasu.ru
Научная электронная библиотека eLIBRARY.RU	Научная электронная библиотека eLIBRARY.RU
Электронно-библиотечная система издательства "Консультант студента"	https://www.studentlibrary.ru/
Электронно-библиотечная система издательства "IPRsmart"	http://www.iprbookshop.ru/
Электронно-библиотечная система издательства "ЮРАЙТ"	https://www.biblio-online.ru/
Электронно-библиотечная система издательства "Лань"	https://e.lanbook.com/
Электронная библиотека Ирбис 64	http://ntb.spbgasu.ru/irbis64r_plus/
Система дистанционного обучения СПбГАСУ Moodle	https://moodle.spbgasu.ru/
Информационно-правовая база данных Кодекс	http://gasudata.lan.spbgasu.ru/docs/
Информационно-правовая система Консультант	\\law.lan.spbgasu.ru\ConsultantPlus ADM
Информационно-правовая система Гарант	\\law.lan.spbgasu.ru\GarantClient

8.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного и свободно распространяемого программного обеспечения

Наименование	Способ распространения (лицензионное или свободно распространяемое)

Microsoft Windows 10 Pro	Договор № Д32009689201 от 18.12.2020г

8.5. Материально-техническое обеспечение дисциплины

Сведения об оснащенности учебных аудиторий и помещений для самостоятельной работы

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность оборудованием и техническими средствами обучения
68. Учебные аудитории для проведения лекционных занятий	Учебная аудитория для проведения занятий лекционного типа, комплект мультимедийного оборудования (персональный компьютер, мультимедийный проектор, экран, аудио-система), доска, экран, комплект учебной мебели, подключение к компьютерной сети СПбГАСУ, выход в Интернет
68. Помещения для самостоятельной работы	Помещение для самостоятельной работы (читальный зал библиотеки, ауд. 217): ПК-23 шт., в т.ч. 1 шт.- ПК для лиц с ОВЗ (системный блок, монитор, клавиатура, мышь) с подключением к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду СПбГАСУ. ПО Microsoft Windows 10
68. Компьютерный класс	Рабочие места с ПК (стол компьютерный, системный блок, монитор, клавиатура, мышь), стол рабочий, подключение к компьютерной сети СПбГАСУ, выход в Internet.

Для инвалидов и лиц с ОВЗ обеспечиваются специальные условия для получения образования в соответствии с требованиями нормативно-правовых документов.