Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Проректор по учебной работе
к.э.н., доцент Изместьев А.А.

17.06.2019г.

Рабочая программа дисциплины
Б1.ДВ.4. Безопасность информационных систем

Направление подготовки: 38.03.02 Менеджмент
Направленность (профиль): Управление бизнесом
Квалификация выпускника: бакалавр
Форма обучения: очная, заочная

	Очная ФО	Заочная ФО
Курс	4	4
Семестр	41	41
Лекции (час)	14	6
Практические (сем, лаб.) занятия (час)	28	10
Самостоятельная работа, включая подготовку к экзаменам и зачетам (час)	102	128
Курсовая работа (час)		
Всего часов	144	144
Зачет (семестр)	41	41
Экзамен (семестр)		

Иркутск 2019

Программа составлена в соответствии с ФГОС ВО по направлению 38.03.02 Менеджмент.

Автор М.М. Бусько

Рабочая программа обсуждена и утверждена на заседании кафедры математики и информатики

Заведующий кафедрой Л.Ю. Волченко

1. Цели изучения дисциплины

Целью освоения дисциплины Безопасность информационных систем является формирование у студентов представления о продуктах и тенденциях развития средств защиты информационных технологий.

Задачи дисциплины:
– сформировать взгляды студентов на безопасность информационных систем как на систематическую научно-практическую деятельность, носящую прикладной характер;
– сформировать у студентов базовые теоретические понятия, лежащие в основе процесса защиты информации;
– дать представление студентам о принципах функционирования и возможностях применения аппаратных средств защиты информации;
– сформировать навыки использования программных и программно-аппаратных средств защиты информации.
– научить студентов использованию криптографических алгоритмов в широко распространенных программных продуктах.

2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Компетенции обучающегося, формируемые в результате освоения дисциплины

Код компетенции по ФГОС ВО	Компетенция
ОПК-7	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ПК-11	владение навыками анализа информации о функционировании системы внутреннего документооборота организации, ведения баз данных по различным показателям и формирования информационного обеспечения участников организационных проектов

Структура компетенции

Компетенция	Формируемые ЗУНы
ОПК-7 способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	З. знать понятийный аппарат и основные категории в области информационно-коммуникационных технологий и основные требования информационной безопасности З. знать подходы к решению стандартные задачи профессиональной деятельности на основе информационной культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности У. уметь осуществлять поиск, обработку и анализ информации о национальной и международной электронной коммерции с учетом основных требований информационной безопасности У. уметь решать стандартные задачи профессиональной деятельности на основе информационной культуры с

	применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности Н. владеть навыками применения технологий и методов проведения исследований в области электронной коммерции и бизнеса, а также обработки полученных результатов с учетом основных требований информационной безопасности Н. владеть навыками применения различных подходов к решению стандартных задач профессиональной деятельности на основе информационной культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ПК-11 владение навыками анализа информации о функционировании системы внутреннего документооборота организации, ведения баз данных по различным показателям и формирования информационного обеспечения участников организационных проектов	З. знать о методах анализа информации и функционировании системы внутреннего документооборота организации, принципах обеспечения информационной безопасности электронных коммерческих процессов, об автоматизированных рабочих местах (АРМ) и особенностях их функционирования У. уметь анализировать информацию, вести баз данных по различным показателям и формировать информационное обеспечение участников организационных проектов Н. владеть навыками анализа информации, ведения баз данных по различным показателям и формирования информационного обеспечения участников организационных проектов

3. Место дисциплины (модуля) в структуре образовательной программы

Принадлежность дисциплины - БЛОК 1 ДИСЦИПЛИНЫ (МОДУЛИ): Дисциплина по выбору.

Предшествующие дисциплины (освоение которых необходимо для успешного освоения данной): "Информационные технологии", "Правовые основы управленческой деятельности"

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

Общая трудоемкость дисциплины составляет 4 зач. ед.,144 часов.

Вид учебной работы	Количество часов (очная ФО)	Количество часов (заочная ФО)
Контактная(аудиторная) работа		
Лекции	14	6
Практические (сем, лаб.) занятия	28	10
Самостоятельная работа, включая подготовку к экзаменам и зачетам	102	128
Всего часов	144	144

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

5.1. Содержание разделов дисциплины

Заочная форма обучения

№ п/п	Раздел и тема дисциплины	Семестр	Лекции	Семинар Лаборат. Практич.	Самостоят. раб.	В интерактивной форме	Формы текущего контроля успеваемости
1	Введение	41	2	0	16		
2	Идентификация пользователей компьютерных систем — субъектов доступа к данным	41	0	2	16		Вопросы для обсуждения на семинарских занятиях
3	Средства и методы ограничения доступа к файлам	41	2	0	16		
4	Программно-аппаратные средства шифрования	41	0	2	16		Вопросы для обсуждения на семинарских занятиях
5	Методы и средства ограничения доступа к компонентам ЭВМ	41	0	2	16		Вопросы для обсуждения на семинарских занятиях
6	Защита программ от несанкционированного копирования	41	0	2	16		Вопросы для обсуждения на семинарских занятиях
7	Хранение и распределение ключевой информации	41	2	0	16		
8	Защита от разрушающих программных воздействий	41	0	2	16		Вопросы для обсуждения на семинарских занятиях
	ИТОГО		6	10	128		

Очная форма обучения

№ п/п	Раздел и тема дисциплины	Семестр	Лекции	Семинар Лаборат. Практич.	Самостоят. раб.	В интерактивной форме	Формы текущего контроля успеваемости
1	Введение	41	1	2	12		Вопросы для обсуждения на семинарских занятиях
2	Идентификация пользователей компьютерных систем	41	1	4	12		Вопросы для обсуждения на семинарских

№ п/п	Раздел и тема дисциплины	Семе-стр	Лек-ции	Семинар Лаборат. Практич.	Само-стоят. раб.	В интера-ктивной форме	Формы текущего контроля успеваемости
	— субъектов доступа к данным						занятиях
3	Средства и методы ограничения доступа к файлам	41	2	4	14		Вопросы для обсуждения на семинарских занятиях
4	Программно-аппаратные средства шифрования	41	2	4	12		Вопросы для обсуждения на семинарских занятиях
5	Методы и средства ограничения доступа к компонентам ЭВМ	41	2	4	14		Вопросы для обсуждения на семинарских занятиях
6	Защита программ от несанкционированного копирования	41	2	4	12		Вопросы для обсуждения на семинарских занятиях
7	Хранение и распределение ключевой информации	41	2	4	14		Вопросы для обсуждения на семинарских занятиях
8	Защита от разрушающих программных воздействий	41	2	2	12		Вопросы для обсуждения на семинарских занятиях
	ИТОГО		14	28	102		

5.2. Лекционные занятия, их содержание

№ п/п	Наименование разделов и тем	Содержание
1	Введение	Предмет и задачи защиты информации в информационных системах. Основные понятия. Уязвимость компьютерных систем. Политика безопасности в компьютерных системах. Оценка защищенности.
2	Идентификация пользователей компьютерных систем — субъектов доступа к данным	Основные понятия и концепции. Идентификация и аутентификация пользователя. Взаимная проверка подлинности пользователей. Протоколы идентификации с нулевой передачей знаний.
3	Средства и методы ограничения доступа к файлам	Защита информации в компьютерных системах от несанкционированного доступа. Система разграничения доступа к информации в компьютерных системах. Управление доступом. Концепция построения систем разграничения доступа (СРД). Организация доступа к ресурсам компьютерных систем. Обеспечение целостности и доступности информации в компьютерных системах.
4	Программно-	Полностью контролируемые компьютерные системы.

№ п/п	Наименование разделов и тем	Содержание
	аппаратные средства шифрования	Основные элементы и средства защиты от несанкционированного доступа. Системы защиты информации от несанкционированного доступа. Система защиты данных Crypton Sigma. СКЗИ «Соболь» для ограничения доступа к компьютеру. СКЗИ «SecretNet» для ограничения доступа к компьютеру.
5	Методы и средства ограничения доступа к компонентам ЭВМ	Защита информации в ПЭВМ. Защита информации, обрабатываемой ПЭВМ и ЛВС, от утечки по сети электропитания. Виды мероприятий по защите информации. Современные системы защиты ПЭВМ от несанкционированного доступа к информации. Особенности построения СКЗИ «Соболь». Особенности построения СКЗИ «Secret Net».
6	Защита программ от несанкционированного копирования	Методы, затрудняющие считывание скопированной информации. Методы, препятствующие использованию скопированной информации. Основные функции средств защиты от копирования. Основные методы защиты от копирования. Методы противодействия динамическим способам снятия защиты программ от копирования.
7	Хранение и распределение ключевой информации	Пароли и ключи. Иерархия ключевой информации. Распределение ключей. Организация хранения ключей. Типовые решения в организации ключевых систем.
8	Защита от разрушающих программных воздействий	Классификация средств исследования программ. Методы защиты программ от исследования. Защита от отладки и дизассемблирования. Общая характеристика и классификация компьютерных вирусов. Общая характеристика средств нейтрализации компьютерных вирусов. Классификация методов защиты от компьютерных вирусов

5.3. Семинарские, практические, лабораторные занятия, их содержание

№ раздела и темы	Содержание и формы проведения
1	Введение в безопасность информационных систем. Устные ответы студентов на контрольные вопросы, обсуждение, дискуссия
2	Идентификация пользователей компьютерных систем — субъектов доступа к данным. Устные ответы студентов на контрольные вопросы, обсуждение, дискуссия
3	Средства и методы ограничения доступа к файлам. Устные ответы студентов на контрольные вопросы, обсуждение, дискуссия
4	Программно-аппаратные средства шифрования. Устные ответы студентов на контрольные вопросы, обсуждение, дискуссия
5	Методы и средства ограничения доступа к компонентам ЭВМ. Устные ответы студентов на контрольные вопросы, обсуждение, дискуссия
6	Защита программ от несанкционированного копирования. Устные ответы студентов на контрольные вопросы, обсуждение, дискуссия
7	Хранение и распределение ключевой информации. Устные ответы студентов на контрольные вопросы, обсуждение, дискуссия

№ раздела и темы	Содержание и формы проведения
8	Защита от разрушающих программных воздействий. Устные ответы студентов на контрольные вопросы, обсуждение, дискуссия

6. Фонд оценочных средств для проведения промежуточной аттестации по дисциплине (полный текст приведен в приложении к рабочей программе)

6.1. Текущий контроль

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1…З.n, У.1…У.n, Н.1…Н.n)	Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы (Наименование оценочного средства)	Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (по 100-балльной шкале)
1	1. Введение	ОПК-7	З.знать понятийный аппарат и основные категории в области информационно-коммуникационных технологий и основные требования информационной безопасности У.уметь осуществлять поиск, обработку и анализ информации о национальной и международной электронной коммерции с учетом основных требований информационной безопасности Н.владеть навыками применения технологий и методов проведения исследований в области электронной коммерции и бизнеса, а также обработки полученных результатов с учетом основных требований информационной безопасности	Вопросы для обсуждения на семинарских занятиях	8-9 балла — сформированные систематические знания; на высоком уровне осуществляемые умения, успешно применяемые навыки; 6-7 балла — сформированные, но содержащие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее отдельные пробелы применение навыков; 3-5 балла — общие, но не структурированные знания; не систематически осуществляемые умения; не систематически применяемые навыки; 2 и менее баллов — студент обнаружил несостоятельност

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1…З.n, У.1…У.n, Н.1…Н.n)	Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы (Наименование оценочного средства)	Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (по 100-балльной шкале)
					ь ответов (9)
2	2. Идентификация пользователей компьютерных систем — субъектов доступа к данным	ПК-11	З.знать о методах анализа информации и функционировании системы внутреннего документооборота организации, принципах обеспечения информационной безопасности электронных коммерческих процессов, об автоматизированных рабочих местах (АРМ) и особенностях их функционирования У.уметь анализировать информацию, вести баз данных по различным показателям и формировать информационное обеспечение участников организационных проектов Н.владеть навыками анализа информации, ведения баз данных по различным показателям и формирования информационного обеспечения участников организационных проектов	Вопросы для обсуждения на семинарских занятиях	12-13 баллов — сформированные систематические знания; на высоком уровне осуществляемые умения, успешно применяемые навыки; 9-11 баллов — сформированные, но содержащие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее отдельные пробелы применение навыков; 5-8 баллов — общие, но не структурированные знания; не систематически осуществляемые умения; не систематически применяемые навыки; 4 и менее баллов — студент обнаружил несостоятельность ответов (13)
3	3. Средства и методы ограничения доступа к файлам	ПК-11	З.знать о методах анализа информации и функционировании системы внутреннего документооборота организации, принципах обеспечения информационной безопасности	Вопросы для обсуждения на семинарских занятиях	12-13 баллов — сформированные систематические знания; на высоком уровне осуществляемые умения, успешно применяемые навыки; 9-11 баллов —

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1…З.n, У.1…У.n, Н.1…Н.n)	Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы (Наименование оценочного средства)	Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (по 100-балльной шкале)
			электронных коммерческих процессов, об автоматизированных рабочих местах (АРМ) и особенностях их функционирования У.уметь анализировать информацию, вести баз данных по различным показателям и формировать информационное обеспечение участников организационных проектов Н.владеть навыками анализа информации, ведения баз данных по различным показателям и формирования информационного обеспечения участников организационных проектов		сформированные, но содержащие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее отдельные пробелы применение навыков; 5-8 баллов — общие, но не структурированные знания; не систематически осуществляемые умения; не систематически применяемые навыки; 4 и менее баллов — студент обнаружил несостоятельность ответов (13)
4	4. Программно-аппаратные средства шифрования	ОПК-7	З.знать подходы к решению стандартные задачи профессиональной деятельности на основе информационной культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности У.уметь решать стандартные задачи профессиональной деятельности на основе	Вопросы для обсуждения на семинарских занятиях	12-13 баллов — сформированные систематические знания; на высоком уровне осуществляемые умения, успешно применяемые навыки; 9-11 баллов — сформированные, но содержащие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1…З.n, У.1…У.n, Н.1…Н.n)	Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы (Наименование оценочного средства)	Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (по 100-балльной шкале)
			информационной культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности Н.владеть навыками применения различных подходов к решению стандартных задач профессиональной деятельности на основе информационной культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности		содержащее отдельные пробелы применение навыков; 5-8 баллов — общие, но не структурированные знания; не систематически осуществляемые умения; не систематически применяемые навыки; 4 и менее баллов — студент обнаружил несостоятельность ответов (13)
5	5. Методы и средства ограничения доступа к компонентам ЭВМ	ПК-11	З.знать о методах анализа информации и функционировании системы внутреннего документооборота организации, принципах обеспечения информационной безопасности электронных коммерческих процессов, об автоматизированных рабочих местах (АРМ) и особенностях их функционирования У.уметь анализировать информацию, вести баз данных по различным показателям и формировать информационное обеспечение	Вопросы для обсуждения на семинарских занятиях	12-13 баллов — сформированные систематические знания; на высоком уровне осуществляемые умения, успешно применяемые навыки; 9-11 баллов — сформированные, но содержащие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее отдельные пробелы применение навыков; 5-8

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1…З.n, У.1…У.n, Н.1…Н.n)	Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы (Наименование оценочного средства)	Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (по 100-балльной шкале)
			участников организационных проектов Н.владеть навыками анализа информации, ведения баз данных по различным показателям и формирования информационного обеспечения участников организационных проектов		баллов — общие, но не структурированные знания; не систематически осуществляемые умения; не систематически применяемые навыки; 4 и менее баллов — студент обнаружил несостоятельность ответов (13)
6	6. Защита программ от несанкционированного копирования	ОПК-7	З.знать понятийный аппарат и основные категории в области информационно-коммуникационных технологий и основные требования информационной безопасности У.уметь осуществлять поиск, обработку и анализ информации о национальной и международной электронной коммерции с учетом основных требований информационной безопасности Н.владеть навыками применения технологий и методов проведения исследований в области электронной коммерции и бизнеса, а также обработки полученных результатов с учетом основных требований информационной безопасности	Вопросы для обсуждения на семинарских занятиях	12-13 баллов — сформированные систематические знания; на высоком уровне осуществляемые умения, успешно применяемые навыки; 9-11 баллов — сформированные, но содержащие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее отдельные пробелы применение навыков; 5-8 баллов — общие, но не структурированные знания; не систематически осуществляемые умения; не систематически применяемые навыки; 4 и менее баллов —

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1…З.n, У.1…У.n, Н.1…Н.n)	Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы (Наименование оценочного средства)	Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (по 100-балльной шкале)
					студент обнаружил несостоятельность ответов (13)
7	7. Хранение и распределение ключевой информации	ПК-11	З.знать о методах анализа информации и функционировании системы внутреннего документооборота организации, принципах обеспечения информационной безопасности электронных коммерческих процессов, об автоматизированных рабочих местах (АРМ) и особенностях их функционирования У.уметь анализировать информацию, вести баз данных по различным показателям и формировать информационное обеспечение участников организационных проектов Н.владеть навыками анализа информации, ведения баз данных по различным показателям и формирования информационного обеспечения участников организационных проектов	Вопросы для обсуждения на семинарских занятиях	12-13 баллов — сформированные систематические знания; на высоком уровне осуществляемые умения, успешно применяемые навыки; 9-11 баллов — сформированные, но содержащие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее отдельные пробелы применение навыков; 5-8 баллов — общие, но не структурированные знания; не систематически осуществляемые умения; не систематически применяемые навыки; 4 и менее баллов — студент обнаружил несостоятельность ответов (13)
8	8. Защита от разрушающих программных воздействий	ОПК-7	З.знать подходы к решению стандартные задачи профессиональной деятельности на основе информационной	Вопросы для обсуждения на семинарских занятиях	12-13 баллов — сформированные систематические знания; на высоком уровне осуществляемые умения, успешно

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1…З.n, У.1…У.n, Н.1…Н.n)	Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы (Наименование оценочного средства)	Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (по 100-балльной шкале)
			культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности У.уметь решать стандартные задачи профессиональной деятельности на основе информационной культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности Н.владеть навыками применения различных подходов к решению стандартных задач профессиональной деятельности на основе информационной культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности		применяемые навыки; 9-11 баллов — сформированные, но содержащие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее отдельные пробелы применение навыков; 5-8 баллов — общие, но не структурированные знания; не систематически осуществляемые умения; не систематически применяемые навыки; 4 и менее баллов — студент обнаружил несостоятельность ответов (13)
				Итого	**100**

6.2. Промежуточный контроль (зачет, экзамен)

Рабочим учебным планом предусмотрен Зачет в семестре 41.

ВОПРОСЫ ДЛЯ ПРОВЕРКИ ЗНАНИЙ:

1-й вопрос билета (30 баллов), вид вопроса: Тест/проверка знаний. Критерий: 27-30 баллов — заслуживает студент, обнаруживший всестороннее, систе-матическое и глубокое знание учебного материала, самостоятельно отве-тивший на вопросы, ответ отличается богатством и точностью использо-ванных терминов, материал излагается последовательно и логично; 21-27 балла — заслуживает студент, обнаруживший полное знание учебного ма-териала, не допускающий в ответе существенных неточностей, самостоя-тельно ответивший на вопросы; 12-21 баллов — заслуживает студент, об-наруживший знание основного учебного материала в объёме, необходи-мом для дальнейшей учебы, однако допустивший некоторые погрешности при ответе на вопросы; 11 и менее — выставляется студенту, обнаружив-шему пробелы в знаниях или отсутствие знаний по значительной части ос-новного учебного материала, допустившему принципиальные ошибки при ответе на вопросы.

Компетенция: ОПК-7 способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Знание: знать подходы к решению стандартные задачи профессиональной деятельности на основе информационной культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

1. Тест: Защита программных средств от исследования
2. Тест: Аппаратно-программные средства защиты информации

Знание: знать понятийный аппарат и основные категории в области информационно-коммуникационных технологий и основные требования информационной безопасности

3. Тест: Защита программ от несанкционированного копирования
4. Тест: Уязвимость компьютерных систем

Компетенция: ПК-11 владение навыками анализа информации о функционировании системы внутреннего документооборота организации, ведения баз данных по различным показателям и формирования информационного обеспечения участников организационных проектов

Знание: знать о методах анализа информации и функционировании системы внутреннего документооборота организации, принципах обеспечения информационной безопасности электронных коммерческих процессов, об автоматизированных рабочих местах (АРМ) и особенностях их функционирования

5. Тест: Защита информации в КС от несанкционированного доступа
6. Тест: Идентификация пользователей КС -- субъектов доступа к данным
7. Тест: Методы и средства ограничения доступа к компонентам ЭВМ
8. Тест: Управление криптографическими ключами

ТИПОВЫЕ ЗАДАНИЯ ДЛЯ ПРОВЕРКИ УМЕНИЙ:

2-й вопрос билета (35 баллов), вид вопроса: Задание на умение. Критерий: 32-35 баллов — заслуживает студент, выполнивший задание в соответ-ствии с заявленной инструкцией или технологией, полностью и правильно; сделаны глубокие и детальные выводы с опорой на источники; имеются ссылки на нормативные документы, не нарушены сроки выполнения зада-ния; 25-32 баллов — заслуживает студент, за правильное выполнение за-дания в соответствии с инструкцией или технологией с учетом 2-3 несуще-ственных ошибок; выводы сформулированы корректно со ссылкой на ис-точники и нормативные документы; сроки выполнения задания не нару-шены; 14-25 — заслуживает студент за выполнение задания правильно не менее чем на половину или если допущена существенная ошибка; выводы сформулированы поверхностно, некорректно; отсутствуют ссылки на ис-точники; сроки выполнения задания не нарушены; 13 и менее — выставля-

ется студенту, если при выполнении задания допущены две (и более) суще-ственные ошибки или задание не выполнено вообще; выводы сформулиро-ваны с грубыми ошибками или отсутствуют вообще; задание выполнено с нарушением сроков..

Компетенция: ОПК-7 способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Умение: уметь осуществлять поиск, обработку и анализ информации о национальной и международной электронной коммерции с учетом основных требований информационной безопасности

Задача № 1. К какому типу информации по ограничению доступа относятся: поря-док передачи служебной информации ограниченного распространения другим организациям.

Задача № 2. К какому типу информации по ограничению доступа относятся: сведе-ния о внутриведомственных и межведомственных обсуждениях, кон-сультациях рабочего и подготовительного характера, включая прото-колы совещаний, служебные записки, справочные и иные материалы, имеющие подготовительный характер, если иное не предусмотрено фе-деральными законами.

Задача № 3. К какому типу информации по ограничению доступа относятся: сведе-ния о деятельности других лиц, полученные государственными органа-ми и органами местного самоуправления при исполнении ими долж-ностных обязанностей, которые составляют коммерческую, банковскую, аудиторскую тайну, тайну кредитных историй; а также тайна следствия и судопроизводства, налоговая тайна, сведения, полученные служащи-ми антимонопольного органа, федерального органа исполнительной власти по рынку ценных бумаг, таможенного органа и др.

Задача № 4. К какому типу информации по ограничению доступа относятся: сведе-ния об авторстве предложений и личных позициях, изложенных в ходе обсуждений, консультаций в процессе работы государственного органа, органа местного самоуправления, за исключением случаев, когда автор публично оглашает данные сведения либо не возражает против раскры-тия сведений о своем авторстве.

Задача № 5. К какому типу информации по ограничению доступа относятся: сведе-ния, связанные с подготовкой проектов индивидуальных правовых и нормативных правовых актов, включая тексты проектов таких актов, если их преждевременное распространение и (или) разглашение нанесет ущерб балансу жизненно важных интересов личности, общества и госу-дарства либо приведет к созданию односторонних преимуществ для субъектов, получивших доступ к указанным сведениям.

Задача № 6. К какому типу информации по ограничению доступа относятся: требо-вания по обеспечению сохранения служебной тайны при выполнении работ на предприятии.

Умение: уметь решать стандартные задачи профессиональной деятельности на основе информационной культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Задача № 7. К какому типу информации по ограничению доступа относятся: сведе-ния о подготовке, принятии и исполнении отдельных решений руковод-ства организации по коммерческим, организационным, производствен-ным, научно-техническим и иным вопросам.

Задача № 8. К какому типу информации по ограничению доступа относятся: сведе-ния о порядке и состоянии охраны, пропускном режиме, системе сигна-лизации, структуре внутренних телефонных линий, условиях и местах хранения материальных ценностей, о транспортных средствах органи-зации, маршрутах передвижения руководства и ответственных сотруд-ников организации.

Задача № 9. К какому типу информации по ограничению доступа относятся: сведе-ния о различных разрабатываемых и реализуемых проектах, планах расширения или

свертывания деятельности организации, о планах ин-вестиций, закупок и продаж и их технико-экономических обоснованиях.
Задача № 10. К какому типу информации по ограничению доступа относятся: сведе-ния о содержании внутренней документации организации (приказов, распоряжений, инструкций, бизнес-планов, информационных и марке-тинговых обзоров).
Задача № 11. К какому типу информации по ограничению доступа относятся: сведе-ния о структуре организации, а также сведения о применяемых методах управления организацией.
Задача № 12. К какому типу информации по ограничению доступа относятся: сведе-ния о структуре организации, производственных мощностях, типе и размещении оборудования, запасах сырья, материалах, комплектую-щих и готовой продукции.

Компетенция: ПК-11 владение навыками анализа информации о функционировании системы внутреннего документооборота организации, ведения баз данных по различным показателям и формирования информационного обеспечения участников организационных проектов

Умение: уметь анализировать информацию, вести баз данных по различным показателям и формировать информационное обеспечение участников организационных проектов
Задача № 13. К какому типу информации по ограничению доступа относятся: о пла-нах строительства Вооруженных Сил Российской Федерации, других войск Российской Федерации, о направлениях развития вооружения и военной техники, о содержании и результатах выполнения целевых программ, научно-исследовательских и опытно-конструкторских работ по созданию и модернизации образцов вооружения и военной техники.
Задача № 14. К какому типу информации по ограничению доступа относятся: о раз-работке, технологии, производстве, об объемах производства, о хране-нии, об утилизации ядерных боеприпасов, их составных частей, деля-щихся ядерных материалов, используемых в ядерных боеприпасах, о технических средствах и (или) методах защиты ядерных боеприпасов от несанкционированного применения, а также о ядерных энергетических и специальных физических установках оборонного значения.
Задача № 15. К какому типу информации по ограничению доступа относятся: о со-держании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому, оперативному и мобилизационному развертыванию Вооруженных Сил Российской Федерации, других войск, воинских формирований и орга-нов, предусмотренных Федеральным законом "Об обороне", об их бое-вой и мобилизационной готовности, о создании и об использовании мо-билизационных ресурсов.
Задача № 16. К какому типу информации по ограничению доступа относятся: о так-тико-технических характеристиках и возможностях боевого применения образцов вооружения и военной техники, о свойствах, рецептурах или технологиях производства новых видов ракетного топлива или взрыв-чатых веществ военного назначения.
Задача № 17. К какому типу информации по ограничению доступа относятся: сведе-ния о внутренних и зарубежных заказчиках, подрядчиках, поставщи-ках, клиентах, потребителях, покупателях, компаньонах, спонсорах, по-средниках и других деловых партнерах организации, а также о ее кон-курентах, которые не содержатся в открытых источниках (справочни-ках, каталогах и т. д.).
Задача № 18. К какому типу информации по ограничению доступа относятся: сведе-ния о материалах и оборудовании, используемом для разработки но-вых продуктов.
Задача № 19. К какому типу информации по ограничению доступа относятся: сведе-ния о планируемой процедуре реорганизации, банкротства или ликви-дации организации.
Задача № 20. К какому типу информации по ограничению доступа относятся: сведе-ния о подготовке и результатах проведения переговоров с деловыми партнерами организации.

Задача № 21. К какому типу информации по ограничению доступа относятся: сведе-ния о применяемых организацией методах изучения рынка, методах маркетинга, о результатах изучения рынка, содержащие оценки состоя-ния и перспективы развития рыночной конъюнктуры.
Задача № 22. К какому типу информации по ограничению доступа относятся: сведе-ния о рыночной стратегии организации.
Задача № 23. К какому типу информации по ограничению доступа относятся: сведе-ния о содержании условий договоров, контрактов, соглашений и дру-гих обязательствах организации;
Задача № 24. К какому типу информации по ограничению доступа относятся: сведе-ния об особенностях конструкторско-технологического, художественно-технического решения продукции, дающие положительный экономиче-ский эффект.

ТИПОВЫЕ ЗАДАНИЯ ДЛЯ ПРОВЕРКИ НАВЫКОВ:

3-й вопрос билета (35 баллов), вид вопроса: Задание на навыки. Критерий: 32-35 баллов — заслуживает студент, выполнивший задание в соответ-ствии с заявленной инструкцией или технологией, полностью и правильно; сделаны глубокие и детальные выводы с опорой на источники; имеются ссылки на нормативные документы, не нарушены сроки выполнения зада-ния; 25-32 баллов — заслуживает студент, за правильное выполнение за-дания в соответствии с инструкцией или технологией с учетом 2-3 несуще-ственных ошибок; выводы сформулированы корректно со ссылкой на ис-точники и нормативные документы; сроки выполнения задания не нару-шены; 14-25 — заслуживает студент за выполнение задания правильно не менее чем на половину или если допущена существенная ошибка; выводы сформулированы поверхностно, некорректно; отсутствуют ссылки на ис-точники; сроки выполнения задания не нарушены; 13 и менее — выставля-ется студенту, если при выполнении задания допущены две (и более) суще-ственные ошибки или задание не выполнено вообще; выводы сформулиро-ваны с грубыми ошибками или отсутствуют вообще; задание выполнено с нарушением сроков..

Компетенция: ОПК-7 способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
Навык: владеть навыками применения различных подходов к решению стандартных задач профессиональной деятельности на основе информационной культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
Задание № 1. В соответствии с методикой ФСТЭК определить степень ущерба, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) информационная си-стема и (или) оператор (обладатель информации) могут выполнять воз-ложенные на них функции с недостаточной эффективностью или выпол-нение функций возможно только с привлечением дополнительных сил и средств.
Задание № 2. В соответствии с методикой ФСТЭК определить степень ущерба, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) информационная си-стема и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций.
Задание № 3. Определить актуальность угрозы с высокой возможностью реализации для ИСПДн, к которой имеют доступ определенные перечнем сотруд-ники организации, являющейся владельцем ИСПДн, либо субъекты ПДн в соответствии с «Требованиями к

защите персональных данных при их обработке в информационных системах персональных данных» (утв. Постановлением Правительства РФ от 01.11.2012 N 1119).
Задание № 4. Определить необходимый уровень защищенности персональных дан-ных в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных» (утв. Постановлением Правительства РФ от 01.11.2012 N 1119). Исход-ные данные задаются преподавателем.
Задание № 5. Определить состав и содержание организационных и технических мер для обеспечения 1 и 2 уровней защищенности персональных данных при их обработке в информационных системах персональных данных в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных» (утв. Постановлением Правительства РФ от 01.11.2012 N 1119).
Задание № 6. Определить состав и содержание организационных и технических мер для обеспечения 3 уровня защищенности персональных данных при их обработке в информационных системах персональных данных в соот-ветствии с «Требованиями к защите персональных данных при их об-работке в информационных системах персональных данных» (утв. По-становлением Правительства РФ от 01.11.2012 N 1119).
Навык: владеть навыками применения технологий и методов проведения исследований в области электронной коммерции и бизнеса, а также обработки полученных результатов с учетом основных требований информационной безопасности
Задание № 7. Определить внутреннего нарушителя информационной безопасности коммерческой тайны в соответствии с методикой ФСТЭК.
Задание № 8. В соответствии с методикой ФСТЭК определить уровень возможностей (потенциал) нарушителя, который является внешним субъектом (физи-ческим лицом), обеспечивающим функционирование информационных систем или обслуживающим инфраструктуру оператора.
Задание № 9. В соответствии с методикой ФСТЭК оценить возможности по реализа-ции угроз безопасности информации внешних нарушителей, не имею-щих права доступа к информационной системе, ее отдельным компо-нентам и реализующих угрозы безопасности информации из-за границ информационной системы.
Задание № 10. В соответствии с методикой ФСТЭК оценить возможности по реализа-ции угроз безопасности информации внутренних нарушителей, имею-щих право постоянного или разового доступа к информационной си-стеме, ее отдельным компонентам.
Задание № 11. В соответствии с методикой ФСТЭК идентифицировать источники угроз безопасности информации для информационных систем, в кото-рых целью защиты является обеспечение целостности и доступности обрабатываемой информации.
Задание № 12. В соответствии с методикой ФСТЭК определить возможные способы реализации угроз безопасности информации пользователями системы непреднамеренно из-за неосторожности или неквалифицированных дей-ствий.
Компетенция: ПК-11 владение навыками анализа информации о функционировании системы внутреннего документооборота организации, ведения баз данных по различным показателям и формирования информационного обеспечения участников организационных проектов
Навык: владеть навыками анализа информации, ведения баз данных по различным показателям и формирования информационного обеспечения участников организационных проектов
Задание № 13. Определить антивирусное программное обеспечение, которое может использоваться в государственных информационных системах 3 класса защищенности в соответствии с «Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государ-ственных информационных системах» (приказ ФСТЭК № 17 от 11.02.2013).
Задание № 14. Определить базовые требования к показателям защищенности средств вычислительной техники 4-го класса согласно РД СВТ.

Задание № 15. Определить класс защищенности информационной системы в соответствии с «Требованиями о защите информации, не составляющей госу-дарственную тайну, содержащейся в государственных информацион-ных системах» (приказ ФСТЭК № 17 от 11.02.2013). Исходные данные задаются преподавателем.
Задание № 16. Определить межсетевые экраны, соответствующие 3 классу защищенно-сти по РД МЭ.
Задание № 17. Определить сертифицированные ФСТЭК операционные системы, соответствующие требованиям 4 класса защищенности средств вычисли-тельной техники (РД СВТ) и имеющие 3 уровень отсутствия недеклари-рованных возможностей (РД НДВ).
Задание № 18. Определить систему обнаружения вторжений, которая может использоваться в государственных информационных системах 4 класса защи-щенности в соответствии с «Требованиями о защите информации, не со-ставляющей государственную тайну, содержащейся в государственных информационных системах» (приказ ФСТЭК № 17 от 11.02.2013).
Задание № 19. Определить состав технических мер защиты информации для информационной системы 3 класса защищенности в соответствии с «Требовани-ями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (приказ ФСТЭК № 17 от 11.02.2013).
Задание № 20. Определить требования к реализации защиты информационной систе-мы, ее средств и систем связи и передачи данных с использованием раз-деления функциональных возможностей по управлению (администри-рованию) информационной системой, управлению (администрирова-нию) системой защиты информации (функций безопасности) и функцио-нальных возможностей пользователей по обработке информации в со-ответствии с «Методическим документом. Меры защиты информации в государственных информационных системах» (утв. ФСТЭК России 11.02.2014).
Задание № 21. Определить требования к реализации защиты машинных носителей информации организацией контроля перемещения используемых в ин-формационной системе машинных носителей информации за пределы контролируемой зоны. в соответствии с «Методическим документом. Меры защиты информации в государственных информационных систе-мах» (утв. ФСТЭК России 11.02.2014).
Задание № 22. Определить требования к реализации обеспечения доступности информации с использованием отказоустойчивых технических средств в соот-ветствии с «Методическим документом. Меры защиты информации в государственных информационных системах» (утв. ФСТЭК России 11.02.2014).
Задание № 23. Определить требования по защите информации от несанкционирован-ного доступа к автоматизированным системам класса защищенности 1А согласно РД АС.
Задание № 24. Определить требования по защите информации от несанкционирован-ного доступа к автоматизированным системам класса защищенности 4А согласно РД АС.

ОБРАЗЕЦ БИЛЕТА

Министерство науки и высшего образования
Российской Федерации
Федеральное государственное бюджетное
образовательное учреждение
высшего образования
«БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «БГУ»)

Направление - 38.03.02 Менеджмент
Профиль - Управление бизнесом
Кафедра математики и информатики
Дисциплина - Безопасность информационных систем

БИЛЕТ № 1

1. Тест (30 баллов).

2. К какому типу информации по ограничению доступа относятся: сведе-ния о внутренних и зарубежных заказчиках, подрядчиках, поставщи-ках, клиентах, потребителях, покупателях, компаньонах, спонсорах, по-средниках и других деловых партнерах организации, а также о ее кон-курентах, которые не содержатся в открытых источниках (справочни-ках, каталогах и т. д.). (35 баллов).
3. Определить требования к реализации защиты машинных носителей ин-формации организацией контроля перемещения используемых в ин-формационной системе машинных носителей информации за пределы контролируемой зоны. в соответствии с «Методическим документом. Меры защиты информации в государственных информационных систе-мах» (утв. ФСТЭК России 11.02.2014). (35 баллов).

Составитель _____ М.М. Бусько

Заведующий кафедрой _____ Л.Ю. Волченко

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

а) основная литература:

1. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации. допущено УМО по образованию в обл. прикладной информатики. учеб. пособие. 3-е изд., перераб. и доп./ Е. К. Баранова, А. В. Бабаш.- М.: ИНФРА-М, 2016.-321 с.
2. Гришина Н. В. Информационная безопасность предприятия. учеб. пособие для вузов. рек. УМО вузов РФ по образованию в обл. историко-архивоведения. 2-е изд., доп./ Н. В. Гришина.- М.: ИНФРА-М, 2017.-238 с.
3. Скрипник Д.А. Обеспечение безопасности персональных данных [Электронный ресурс]/ Скрипник Д.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 121 с.— Режим доступа: http://www.iprbookshop.ru/52153.— ЭБС «IPRbooks»
4. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 702 с. — 978-5-4488-0070-2. — Режим доступа: http://www.iprbookshop.ru/63594.html

б) дополнительная литература:

1. Астахова А. В. Информационные системы в экономике и защита информации на предприятиях-участниках ВЭД. учеб. пособие для вузов/ А. В. Астахова.- СПб.: Троицкий мост, 2014.-214 с.
2. Гугуева Т. А. Конфиденциальное делопроизводство. рек. УМО по образованию в обл. менеджмента. учеб. пособие для вузов/ Т. А. Гугуева.- М.: ИНФРА-М, 2015.-191 с.
3. Банк данных угроз безопасности информации. Федеральная служба по техническому и экспортному контролю. Государственный научно-исследовательский испытательный институт проблем технической защиты информации. http://bdu.fstec.ru/ (30.08.2017)
4. Галатенко В.А. Основы информационной безопасности [Электронный ресурс]/ В.А. Галатенко— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 266 с.— Режим доступа: http://www.iprbookshop.ru/52209.html.— ЭБС «IPRbooks» [08.09.2017]
5. Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00. http://fstec.ru/component/attachments/download/489

6. Коваленко Ю.И. Методика защиты информации в организациях [Электронный ресурс]: монография/ Ю.И. Коваленко, Г.И. Москвитин, М.М. Тараскин— Электрон. текстовые данные.— М.: Русайнс, 2016.— 162 с.— Режим доступа: http://www.iprbookshop.ru/61625.html.— ЭБС «IPRbooks» [08.09.2017]
7. Перечень средств защиты информации, сертифицированных ФСБ России. http://clsz.fsb.ru/files/download/svedenia_po_sertifikatam_(010717).doc
8. Рагозин Ю.Н. Инженерно-техническая защита информации [Электронный ресурс] : учебное пособие по физическим основам образования технических каналов утечки информации и по практикуму оценки их опасности / Ю.Н. Рагозин. — Электрон. текстовые данные. — СПб. : Интермедия, 2018. — 168 c. — 978-5-4383-0161-5. — Режим доступа: http://www.iprbookshop.ru/73641.html

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля), включая профессиональные базы данных и информационно-справочные системы

Для освоения дисциплины обучающемуся необходимы следующие ресурсы информационно-телекоммуникационной сети «Интернет»:

– Сайт Байкальского государственного университета, адрес доступа: http://bgu.ru/, доступ круглосуточный неограниченный из любой точки Интернет

– ИВИС - Универсальные базы данных, адрес доступа: http://www.dlib.eastview.ru/. доступ круглосуточный неограниченный из любой точки Интернет при условии регистрации в БГУ

– КиберЛенинка, адрес доступа: http://cyberleninka.ru. доступ круглосуточный, неограниченный для всех пользователей, бесплатное чтение и скачивание всех научных публикаций, в том числе пакет «Юридические науки», коллекция из 7 журналов по правоведению

– Научная электронная библиотека eLIBRARY.RU, адрес доступа: http://elibrary.ru/. доступ к российским журналам, находящимся полностью или частично в открытом доступе при условии регистрации

– Национальный цифровой ресурс «Руконт», адрес доступа: http://www.rucont.ru. доступ неограниченный

– Федеральная служба безопасности Российской Федерации, адрес доступа: http://fsb.ru. доступ неограниченный

– Федеральная служба по техническому и экспортному контролю, адрес доступа: http://fstec.ru. доступ неограниченный

– Федеральный образовательный портал «Экономика, Социология, Менеджмент», адрес доступа: http://www.ecsocman.edu.ru. доступ неограниченный

– ЭБС BOOK.ru - электронно-библиотечная система от правообладателя, адрес доступа: http://www.book.ru/. доступ неограниченный

– Электронная библиотека Издательского дома "Гребенников", адрес доступа: http://www.grebennikon.ru/. доступ с компьютеров сети БГУ (по IP-адресам)

– Электронно-библиотечная система IPRbooks, адрес доступа: http://www.iprbookshop.ru. доступ неограниченный

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Изучать дисциплину рекомендуется в соответствии с той последовательностью, которая обозначена в ее содержании. Для успешного освоения курса обучающиеся должны иметь первоначальные знания в области информационных технологий.

На лекциях преподаватель озвучивает тему, знакомит с перечнем литературы по теме, обосновывает место и роль этой темы в данной дисциплине, раскрывает ее практическое значение. В ходе лекций студенту необходимо вести конспект, фиксируя основные понятия и проблемные вопросы.

Практические (семинарские) занятия по своему содержанию связаны с тематикой лекционных занятий. Начинать подготовку к занятию целесообразно с конспекта лекций. Задание на практическое (семинарское) занятие сообщается обучающимся до его проведения. На семинаре преподаватель организует обсуждение этой темы, выступая в качестве организатора, консультанта и эксперта учебно-познавательной деятельности обучающегося.

Изучение дисциплины (модуля) включает самостоятельную работу обучающегося.

Основными видами самостоятельной работы студентов с участием преподавателей являются:

• текущие консультации;

• коллоквиум как форма контроля освоения теоретического содержания дисциплин: (в часы консультаций, предусмотренные учебным планом);

• прием и разбор домашних заданий (в часы практических занятий);

• прием и защита лабораторных работ (во время проведения занятий);

• выполнение курсовых работ в рамках дисциплин (руководство, консультирование и защита курсовых работ в часы, предусмотренные учебным планом) и др.

Основными видами самостоятельной работы студентов без участия преподавателей являются:

• формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);

• самостоятельное изучение отдельных тем или вопросов по учебникам или учебным пособиям;

• написание рефератов, докладов;

• подготовка к семинарам и лабораторным работам;

• выполнение домашних заданий в виде решения отдельных задач, проведения типовых расчетов, расчетно-компьютерных и индивидуальных работ по отдельным разделам содержания дисциплин и др.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

В учебном процессе используется следующее программное обеспечение:

– MS Office,

– Гарант платформа F1 7.08.0.163 - информационная справочная система,

– КонсультантПлюс: Версия Проф - информационная справочная система,

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю):

В учебном процессе используется следующее оборудование:

– Помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду вуза,

– Учебные аудитории для проведения: занятий лекционного типа, занятий семинарского типа, практических занятий, выполнения курсовых работ, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованные специализированной мебелью и техническими средствами обучения,

– Компьютерный класс,

– Наборы демонстрационного оборудования и учебно-наглядных пособий