Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Проректор по учебной работе
д.э.н., доц. Бубнов В.А

_____

22.06.2020г.

Рабочая программа дисциплины
Б1.ДВ.3. Информационная безопасность

Направление подготовки: 38.03.05 Бизнес-информатика
Направленность (профиль): Цифровая экономика
Квалификация выпускника: бакалавр
Форма обучения: очная

Курс	2
Семестр	21
Лекции (час)	28
Практические (сем, лаб.) занятия (час)	28
Самостоятельная работа, включая подготовку к экзаменам и зачетам (час)	88
Курсовая работа (час)	
Всего часов	144
Зачет (семестр)	
Экзамен (семестр)	21

Иркутск 2020

Программа составлена в соответствии с ФГОС ВО по направлению 38.03.05 Бизнес-информатика.

Автор М.М. Бусько

Рабочая программа обсуждена и утверждена на заседании кафедры математических методов и цифровых технологий

Заведующий кафедрой А.В. Родионов

Дата актуализации рабочей программы: 30.06.2021

1. Цели изучения дисциплины

Цель курса — изучение комплекса проблем информационной безопасности организаций различных типов и направлений деятельности; построения, функционирования и совершенствования правовых, организационных, технических и технологических процессов, обеспечивающих информационную безопасность и формирующих структуру системы защиты ценной и конфиденциальной информации; изучение понятий и видов защищаемой информации по законодательству РФ, системы защиты государственной тайны.

Задачи курса:

- овладение теоретическими, практическими и методическими вопросами обеспечения информационной безопасности;
- освоение системных комплексных методов защиты информации от различных видов объективных и субъективных угроз в процессе ее возникновения, обработки, использования и хранения;
- ознакомление с современными законодательными и нормативно-правовыми проблемами обеспечения информационной безопасности;
- приобретение теоретических и практических навыков по основам использования современных методов правовой защиты государственной, коммерческой, служебной, профессиональной и личной тайны, персональных данных в компьютерных системах;
- лицензирования и сертификации в области защиты информации;
- формирование практических навыков и способностей осуществления мероприятий по обеспечению правовой защиты информации.

Изучаемые вопросы рассматриваются в широком диапазоне современных проблем и затрагивают предметные сферы защиты как документированной информации (на бумажных и технических носителях), циркулирующей в традиционном или электронном документообороте, находящейся в компьютерных системах, так и недокументированной информации, распространяемой персоналом в процессе управленческой (деловой) или производственной деятельности.

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
ОК-4	способность использовать основы правовых знаний в различных сферах деятельности
ОПК-1	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-9	организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия

Структура компетенции

Компетенция	Формируемые ЗУНы
ОК-4 способность использовать основы правовых знаний в различных сферах деятельности	З. Знать общие положения теории права и основных отраслей права в различных сферах деятельности У. Уметь применять правовые знания в различных сферах

	деятельности Н. Иметь навык применения основ правовых знаний в различных сферах деятельности
ОПК-1 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. Знает, как решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности У. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности Н. Владеет навыками решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ПК-9 организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия	З. Знает, как организовать взаимодействие с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия У. Умеет организовать взаимодействие с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия Н. Владеет навыками организации взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия

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): "Правоведение", "Программирование", "Информационные системы и технологии"

Дисциплины, использующие знания, умения, навыки, полученные при изучении данной: "Информационное право", "Основы построения информационных систем", "Проектирование информационных систем", "Распределенные системы"

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

Контактная(аудиторная) работа	
Лекции	28
Практические (сем, лаб.) занятия	28
Самостоятельная работа, включая подготовку к экзаменам и зачетам	88
Всего часов	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

№ п/п	Раздел и тема дисциплины	Семестр	Лекции	Семинар Лаборат. Практич.	Самостоят. раб.	В интерактивной форме	Формы текущего контроля успеваемости
1	Тема 1. Основы информационной безопасности	21	4	4	12		Практическая работа №1
2	Тема 2. Правовая защита информации	21	4	4	14		Практическая работа №2
3	Тема 3. Организационная защита информации	21	4	4	12		Практическая работа №3
4	Тема 4. Защита информации в компьютерных информационных системах	21	4	4	12		Практическая работа №4
5	Тема 5. Криптографические методы защиты информации	21	4	4	12		Практическая работа №5
6	Тема 6. Защита от вредоносного программного обеспечения и спама	21	4	4	14		Практическая работа №6
7	Тема 7. Инженерно-технические методы защиты информации	21	4	4	12		Практическая работа №7
	ИТОГО		28	28	88		

5.2. Лекционные занятия, их содержание

№ п/п	Наименование разделов и тем	Содержание
1.1	Основы информационной безопасности	Понятие информационной безопасности. Актуальность информационной безопасности. Принципы обеспечения информационной безопасности. Структура информационной безопасности.
1.2	Система защиты информации	Структура системы защиты информации РФ. Угрозы безопасности в информационной сфере. Комплексный подход

№ п/п	Наименование разделов и тем	Содержание
		к защите информации.
2.1	Правовая защита интересов личности, общества и государства от информационных угроз	Структура нормативной базы Российской Федерации по вопросам информационной безопасности. Правовая защита интересов личности, общества и государства от информационных угроз. Лицензирование, сертификация и аттестация в сфере защиты информации.
2.2	Защита информации по режиму доступа	Классификация информации по видам тайны и степеням конфиденциальности. Защита государственной тайны. Защита коммерческой тайны. Защита персональных данных.
3.1	Организационная защита информации	Организационная защита информации. Зоны ответственности. Локальные нормативные акты в области информационной безопасности. Организация службы безопасности предприятия.
3.2	Организация конфиденциального документооборота	Грифы ограничения доступа к документам. Организация конфиденциального документооборота. Стандарты и спецификации в области информационной безопасности.
4.1	Защита информации в компьютерных системах	Анализ угроз информационной безопасности компьютерных систем. Технологии защиты информации в компьютерных системах. Идентификация, аутентификация и управление доступом. Обеспечение безопасности операционных систем.
4.2	Безопасность межсетевого обмена данными	Технологии межсетевого экранирования. Технологии виртуальных защищенных сетей (VPN). Анализ защищенности и обнаружение атак. Технологии резервного копирования и восстановления данных.
5.1	Методы криптографического преобразования информации	Классификация методов криптографического закрытия информации. Симметричные криптосистемы. Криптосистемы с открытым ключом.
5.2	Практическое применение криптографии	Квантовая криптография. Стеганография. Электронная подпись.
6.1	Вредоносное программное обеспечение	Условия существования вредоносных программ. Классификация вредоносных программ.
6.2	Защита компьютерных систем от воздействия вредоносных программ	Основы работы антивирусных программ. Защита компьютерных систем от воздействия вредоносных программ. Защита от СПАМА.
7.1	Инженерно-техническая защита информации	Инженерно-техническая защита информации. Технические каналы утечки информации. Средства выявления каналов утечки информации.
7.2	Методы и способы защиты информации от утечки по техническим каналам	Методы и способы защиты информации от утечки по техническим каналам. Физическая укрепленность объекта информатизации.

5.3. Семинарские, практические, лабораторные занятия, их содержание

№ раздела и темы	Содержание и формы проведения
1	Семинар 1. Выполнение практической работы №1
1	Семинар 2. Защита отчета по практической работе №1
2	Семинар 3. Выполнение практической работы №2
2	Семинар 4. Защита отчета по практической работе №2
3	Семинар 5. Выполнение практической работы №3
3	Семинар 6. Защита отчета по практической работе №3
4	Семинар 7. Выполнение практической работы №4
4	Семинар 8. Защита отчета по практической работе №4
5	Семинар 9. Выполнение практической работы №5
5	Семинар 10. Защита отчета по практической работе №5
6	Семинар 11. Выполнение практической работы №6
6	Семинар 12. Защита отчета по практической работе №6
7	Семинар 13. Выполнение практической работы №7
7	Семинар 14. Защита отчета по практической работе №7

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. Тема 1. Основы информационной безопасности	ПК-9	З.Знает, как организовать взаимодействие с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия У.Умеет организовать взаимодействие с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия Н.Владеет навыками организации	Практическая работа №1	9-10 баллов — сформированные систематические знания; на высоком уровне осуществляе-мые умения, успешно применяемые навыки; 7-8 баллов — сформированные, но содержащие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее отдельные

№ 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)
			взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия		пробелы применение навыков; 5-6 баллов — общие, но не структурированные знания; не систематически осуществляемые умения; не систематически применяемые навыки; 4 и менее баллов — студент обнаружил несостоятельность ответов (10)
2	2. Тема 2. Правовая защита информации	ОК-4	З.Знать общие положения теории права и основных отраслей права в различных сферах деятельности У.Уметь применять правовые знания в различных сферах деятельности Н.Иметь навык применения основ правовых знаний в различных сферах деятельности	Практическая работа №2	14-15 баллов — сформированные систематические знания; на высоком уровне осуществляемые умения, успешно применяемые навыки; 11-13 баллов — сформированные, но содержащие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее отдельные пробелы применение навыков; 7-10 баллов — общие, но не структурированные знания; не систематически осуществляемые умения; не

№ 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)
					систематически применяемые навыки; 6 и менее баллов — студент обнаружил несостоятель-ность ответов (15)
3	3. Тема 3. Организационная защита информации	ОК-4	З.Знать общие положения теории права и основных отраслей права в различных сферах деятельности У.Уметь применять правовые знания в различных сферах деятельности Н.Иметь навык применения основ правовых знаний в различных сферах деятельности	Практическая работа №3	14-15 баллов — сформированные систематические знания; на высоком уровне осуществляе-мые умения, успешно применяемые навыки; 11-13 баллов — сформированные, но содержа-щие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы уме-ния; в целом успешное, но содержащее отдельные пробелы применение навыков; 7-10 баллов — общие, но не структурированн ые знания; не систематически осуществляемые умения; не систематически применяемые навыки; 6 и менее баллов — студент обнаружил несостоятель-ность ответов (15)
4	4. Тема 4. Защита	ПК-9	З.Знает, как	Практическая работа	14-15 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)
	информации в компьютерных информационных системах		организовать взаимодействие с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия У.Умеет организовать взаимодействие с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия Н.Владеет навыками организации взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия	№4	сформированные систематические знания; на высоком уровне осуществляе-мые умения, успешно применяемые навыки; 11-13 баллов — сформированные, но содержа-щие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы уме-ния; в целом успешное, но содержащее отдельные пробелы применение навыков; 7-10 баллов — общие, но не структурированн ые знания; не систематически осуществляемые умения; не систематически применяемые навыки; 6 и менее баллов — студент обнаружил несостоятель-ность ответов (15)
5	5. Тема 5. Криптографическ ие методы защиты информации	ОПК-1	З.Знает, как решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных	Практическая работа №5	14-15 баллов — сформированные систематические знания; на высоком уровне осуществляе-мые умения, успешно применяемые навыки; 11-13 баллов — сформированные,

№ 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)
			технологий и с учетом основных требований информационной безопасности У.Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности Н.Владеет навыками решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности		но содержа-щие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы уме-ния; в целом успешное, но содержащее отдельные пробелы применение навыков; 7-10 баллов — общие, но не структурированн ые знания; не систематически осуществляемые умения; не систематически применяемые навыки; 6 и менее баллов — студент обнаружил несостоятель-ность ответов (15)
6	6. Тема 6. Защита от вредоносного программного обеспечения и спама	ОПК-1	З.Знает, как решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности У.Умеет решать стандартные задачи	Практическая работа №6	14-15 баллов — сформированные систематические знания; на высоком уровне осуществляе-мые умения, успешно применяемые навыки; 11-13 баллов — сформированные, но содержа-щие отдельные пробелы знания; в целом успешные, но содержащие

№ 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)
			профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности Н.Владеет навыками решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности		отдельные пробелы уме-ния; в целом успешное, но содержащее отдельные пробелы применение навыков; 7-10 баллов — общие, но не структурированн ые знания; не систематически осуществляемые умения; не систематически применяемые навыки; 6 и менее баллов — студент обнаружил несостоятель-ность ответов (15)
7	7. Тема 7. Инженерно-технические методы защиты информации	ПК-9	З.Знает, как организовать взаимодействие с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия У.Умеет организовать взаимодействие с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия Н.Владеет навыками организации	Практическая работа №7	14-15 баллов — сформированные систематические знания; на высоком уровне осуществляе-мые умения, успешно применяемые навыки; 11-13 баллов — сформированные, но содержа-щие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы уме-ния; в целом успешное, но содержащее отдельные

№ 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)
			взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия		пробелы применение навыков; 7-10 баллов — общие, но не структурированные знания; не систематически осуществляемые умения; не систематически применяемые навыки; 6 и менее баллов — студент обнаружил несостоятель-ность ответов (15)
				Итого	**100**

6.2. Промежуточный контроль (зачет, экзамен)

Рабочим учебным планом предусмотрен Экзамен в семестре 21.

ВОПРОСЫ ДЛЯ ПРОВЕРКИ ЗНАНИЙ:

1-й вопрос билета (30 баллов), вид вопроса: Тест/проверка знаний. Критерий: Максимальное количество баллов, которые может получить каждый студент за тест в относительных единицах равняется 30-ти. Каждый правильный ответ оценивается в 1 балл, полученный результат делится на общее количество вопросов в тесте и умножится на 30..

Компетенция: ОК-4 способность использовать основы правовых знаний в различных сферах деятельности

Знание: Знать общие положения теории права и основных отраслей права в различных сферах деятельности

1. Анализ угроз информационной безопасности компьютерных систем.
2. Грифы ограничения доступа к документам.
3. Защита государственной тайны.
4. Защита коммерческой тайны.
5. Защита персональных данных.
6. Классификация информации по видам тайны и степеням конфиденциальности.
7. Локальные нормативные акты в области информационной безопасности.
8. Организационная защита информации. Зоны ответственности.
9. Организация конфиденциального документооборота.

10. Организация службы безопасности предприятия.
11. Правовая защита интересов личности, общества и государства от информационных угроз.
12. Структура нормативной базы Российской Федерации по вопросам информационной безопасности.

Компетенция: ОПК-1 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: Знает, как решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

13. Защита компьютерных систем от воздействия вредоносных программ.
14. Защита от СПАМА.
15. Квантовая криптография.
16. Классификация вредоносных программ.
17. Классификация методов криптографического закрытия информации.
18. Криптосистемы с открытым ключом.
19. Основы работы антивирусных программ.
20. Симметричные криптосистемы.
21. Стеганография.
22. Условия существования вредоносных программ.
23. Электронная подпись.

Компетенция: ПК-9 организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия

Знание: Знает, как организовать взаимодействие с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия

24. Актуальность информационной безопасности.
25. Анализ защищенности и обнаружение атак.
26. Идентификация, аутентификация и управление доступом.
27. Инженерно-техническая защита информации.
28. Методы и способы защиты информации от утечки по техническим каналам.
29. Обеспечение безопасности операционных систем.
30. Понятие информационной безопасности.
31. Принципы обеспечения информационной безопасности.
32. Средства выявления каналов утечки информации.
33. Структура информационной безопасности.
34. Структура системы защиты информации РФ.
35. Технические каналы утечки информации.
36. Технологии виртуальных защищенных сетей (VPN).
37. Технологии защиты информации в компьютерных системах.
38. Технологии межсетевого экранирования.
39. Технологии резервного копирования и восстановления данных.
40. Угрозы безопасности в информационной сфере.
41. Физическая укрепленность объекта информатизации.

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 соответствии 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 задания; 25-32 баллов — заслуживает студент, за правильное выполнение задания в соответствии с инструкцией или технологией с учетом 2-3 несущественных ошибок; выводы сформулированы корректно со ссылкой на источники и нормативные документы; сроки выполнения задания не нарушены; 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 источники; сроки выполнения задания не нарушены; 13 и менее — выставляется студенту, если при выполнении задания допущены две (и более) существенные ошибки или задание не выполнено вообще; выводы сформулированы с грубыми ошибками или отсутствуют вообще; задание выполнено с нарушением сроков..

Компетенция: ОК-4 способность использовать основы правовых знаний в различных сферах деятельности

Умение: Уметь применять правовые знания в различных сферах деятельности

Задача № 1. К какому типу информации по ограничению доступа относятся: информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну).

Задача № 2. К какому типу информации по ограничению доступа относятся: порядок передачи служебной информации ограниченного распространения другим организациям.

Задача № 3. К какому типу информации по ограничению доступа относятся: сведения о внутриведомственных и межведомственных обсуждениях, консультациях рабочего и подготовительного характера, включая протоколы совещаний, служебные записки, справочные и иные материалы, имеющие подготовительный характер, если иное не предусмотрено федеральными законами.

Задача № 4. К какому типу информации по ограничению доступа относятся: сведения о деятельности других лиц, полученные государственными органами и органами местного самоуправления при исполнении ими должностных обязанностей, которые составляют коммерческую, банковскую, аудиторскую тайну, тайну кредитных историй; а также тайна следствия и судопроизводства, налоговая тайна, сведения, полученные служащими антимонопольного органа, федерального органа исполнительной власти по рынку ценных бумаг, таможенного органа и др.

Задача № 5. К какому типу информации по ограничению доступа относятся: сведения о порядке и состоянии охраны, пропускном режиме, системе сигнализации, структуре внутренних телефонных линий, условиях и местах хранения материальных ценностей, о транспортных средствах организации, маршрутах передвижения руководства и ответственных сотрудников организации.

Задача № 6. К какому типу информации по ограничению доступа относятся: сведения о структуре организации, производственных мощностях, типе и размещении оборудования, запасах сырья, материалах, комплектующих и готовой продукции.

Задача № 7. К какому типу информации по ограничению доступа относятся: сведения 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 раскрытия сведений о своем авторстве.

Задача № 8. К какому типу информации по ограничению доступа относятся: требования по обеспечению сохранения служебной тайны при выполнении работ на предприятии.

Компетенция: ОПК-1 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: Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Задача № 9. К какому типу информации по ограничению доступа относятся: сведения о внутренних и зарубежных заказчиках, подрядчиках, поставщиках, клиентах, потребителях, покупателях, компаньонах, спонсорах, посредниках и других деловых партнерах организации, а также о ее конкурентах, которые не содержатся в открытых источниках (справочниках, каталогах и т. д.).

Задача № 10. К какому типу информации по ограничению доступа относятся: сведения о планируемой процедуре реорганизации, банкротства или ликвидации организации.

Задача № 11. К какому типу информации по ограничению доступа относятся: сведения о подготовке, принятии и исполнении отдельных решений руководства организации по коммерческим, организационным, производственным, научно-техническим и иным вопросам.

Задача № 12. К какому типу информации по ограничению доступа относятся: сведения о применяемых организацией методах изучения рынка, методах маркетинга, о результатах изучения рынка, содержащие оценки состояния и перспективы развития рыночной конъюнктуры.

Задача № 13. К какому типу информации по ограничению доступа относятся: сведения о различных разрабатываемых и реализуемых проектах, планах расширения или свертывания деятельности организации, о планах инвестиций, закупок и продаж и их технико-экономических обоснованиях.

Задача № 14. К какому типу информации по ограничению доступа относятся: сведения о содержании внутренней документации организации (приказов, распоряжений, инструкций, бизнес-планов, информационных и маркетинговых обзоров).

Задача № 15. К какому типу информации по ограничению доступа относятся: сведения о содержании условий договоров, контрактов, соглашений и других обязательствах организации;

Задача № 16. К какому типу информации по ограничению доступа относятся: сведения о структуре организации, а также сведения о применяемых методах управления организацией.

Компетенция: ПК-9 организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия

Умение: Умеет организовать взаимодействие с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия

Задача № 17. К какому типу информации по ограничению доступа относятся: информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией.

Задача № 18. К какому типу информации по ограничению доступа относятся: о планах 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 № 19. К какому типу информации по ограничению доступа относятся: о разработке, технологии, производстве, об объемах производства, о хранении, об утилизации ядерных боеприпасов, их составных частей, делящихся 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 № 20. К какому типу информации по ограничению доступа относятся: о тактико-технических характеристиках и возможностях боевого применения образцов вооружения и военной техники, о свойствах, рецептурах или технологиях производства новых видов ракетного топлива или взрывчатых веществ военного назначения.
Задача № 21. К какому типу информации по ограничению доступа относятся: сведения о материалах и оборудовании, используемом для разработки новых продуктов.
Задача № 22. К какому типу информации по ограничению доступа относятся: сведения о подготовке и результатах проведения переговоров с деловыми партнерами организации.
Задача № 23. К какому типу информации по ограничению доступа относятся: сведения о рыночной стратегии организации.
Задача № 24. К какому типу информации по ограничению доступа относятся: сведения об особенностях конструкторско-технологического, художественно-технического решения продукции, дающие положительный экономический 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 соответствии 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 задания; 25-32 баллов — заслуживает студент, за правильное выполнение задания в соответствии с инструкцией или технологией с учетом 2-3 несущественных ошибок; выводы сформулированы корректно со ссылкой на источники и нормативные документы; сроки выполнения задания не нарушены; 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 источники; сроки выполнения задания не нарушены; 13 и менее — выставляется студенту, если при выполнении задания допущены две (и более) существенные ошибки или задание не выполнено вообще; выводы сформулированы с грубыми ошибками или отсутствуют вообще; задание выполнено с нарушением сроков..

Компетенция: ОК-4 способность использовать основы правовых знаний в различных сферах деятельности
Навык: Иметь навык применения основ правовых знаний в различных сферах деятельности
Задание № 1. Для определенного объекта защиты информации необходимо провести анализ его защищенности и определить источники появления угроз. Объект: Веб-сервер.
Задание № 2. Для определенного объекта защиты информации необходимо провести анализ его защищенности и определить источники появления угроз. Объект: Компьютерная сеть материальной группы.
Задание № 3. Для определенного объекта защиты информации необходимо провести анализ его защищенности и определить источники появления угроз. Объект: Одиночно стоящий компьютер в бухгалтерии.
Задание № 4. Для определенного объекта защиты информации необходимо провести анализ его защищенности и определить источники появления угроз. Объект: Одноранговая локальная сеть без выхода в Интернет.

Задание № 5. Для определенного объекта защиты информации необходимо провести анализ его защищенности и определить источники появления угроз. Объект: Одноранговая локальная сеть с выходом в Интернет.
Задание № 6. Для определенного объекта защиты информации необходимо провести анализ его защищенности и определить источники появления угроз. Объект: Почтовый сервер.
Задание № 7. Для определенного объекта защиты информации необходимо провести анализ его защищенности и определить источники появления угроз. Объект: Сеть с выделенным сервером без выхода в Интернет.
Задание № 8. Для определенного объекта защиты информации необходимо провести анализ его защищенности и определить источники появления угроз. Объект: Сеть с выделенным сервером с выхода в Интернет.

Компетенция: ОПК-1 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: Владеет навыками решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
Задание № 9. Для определенного объекта защиты информации необходимо провести анализ его защищенности и определить источники появления угроз. Объект: Комната для переговоров по сделкам на охраняемой террито-рии.
Задание № 10. Для определенного объекта защиты информации необходимо провести анализ его защищенности и определить источники появления угроз. Объект: Компьютер, хранящий конфиденциальную информацию о раз-работках предприятия.
Задание № 11. Для определенного объекта защиты информации необходимо провести анализ его защищенности и определить источники появления угроз. Объект: Компьютер, хранящий конфиденциальную информацию о со-трудниках предприятия.
Задание № 12. Для определенного объекта защиты информации необходимо провести анализ его защищенности и определить источники появления угроз. Объект: Материалы для служебного пользования на твердых носителях в архиве.
Задание № 13. Для определенного объекта защиты информации необходимо провести анализ его защищенности и определить источники появления угроз. Объект: Материалы для служебного пользования на твердых носителях и на электронных носителях в налоговой инспекции.
Задание № 14. Для определенного объекта защиты информации необходимо провести анализ его защищенности и определить источники появления угроз. Объект: Материалы для служебного пользования на твердых носителях и на электронных носителях на закрытом предприятии.
Задание № 15. Для определенного объекта защиты информации необходимо провести анализ его защищенности и определить источники появления угроз. Объект: Средства телекоммуникации (радиотелефоны, мобильные теле-фоны).
Задание № 16. Для определенного объекта защиты информации необходимо провести анализ его защищенности и определить источники появления угроз. Объект: Телефонная база данных (содержащая и информацию ограни-ченного пользования) в твердой копии и на электронных носителях.

Компетенция: ПК-9 организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия

Навык: Владеет навыками организации взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия

Задание № 17. Для определенного объекта защиты информации необходимо провести анализ его защищенности и определить источники появления угроз. Объект: Комната для переговоров по сделкам на неохраняемой терри-тории.

Задание № 18. Для определенного объекта защиты информации необходимо провести анализ его защищенности и определить источники появления угроз. Объект: Материалы для служебного пользования на твердых носителях и на электронных носителях в производстве.

Задание № 19. Для определенного объекта защиты информации необходимо провести анализ его защищенности и определить источники появления угроз. Объект: Материалы по владельцам автомобилей (твердая копия, фото-графии, электронные носители и др.).

Задание № 20. Для определенного объекта защиты информации необходимо провести анализ его защищенности и определить источники появления угроз. Объект: Материалы по недвижимости (твердая копия, фотографии, электронные носители и др.).

Задание № 21. Для определенного объекта защиты информации необходимо провести анализ его защищенности и определить источники появления угроз. Объект: Партийные списки и руководящие документы (твердая копия и на электронных носителях).

Задание № 22. Для определенного объекта защиты информации необходимо провести анализ его защищенности и определить источники появления угроз. Объект: Сведения по общественно-полезным организациям (красный крест и др.) (твердая копия и на электронных носителях).

Задание № 23. Для определенного объекта защиты информации необходимо провести анализ его защищенности и определить источники появления угроз. Объект: Сведения по тоталитарным сектам и другим общественно-вредным организациям (твердая копия и на электронных носителях).

Задание № 24. Для определенного объекта защиты информации необходимо провести анализ его защищенности и определить источники появления угроз. Объект: Судебные материалы (твердая копия и на электронных носите-лях).

ОБРАЗЕЦ БИЛЕТА

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

Направление - 38.03.05 Бизнес-информатика
Профиль - Цифровая экономика
Кафедра математических методов и цифровых технологий
Дисциплина - Информационная безопасность

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Тест (30 баллов).
2. К какому типу информации по ограничению доступа относятся: сведения о применяемых организацией методах изучения рынка, методах маркетинга, о результатах изучения рынка, содержащие оценки состояния и перспективы развития рыночной конъюнктуры. (35 баллов).
3. Для определенного объекта защиты информации необходимо провести анализ его защищенности и определить источники появления угроз. Объект: Материалы

для служебного пользования на твердых носителях и на электронных носителях в производстве. (35 баллов).

Составитель _____ М.М. Бусько

Заведующий кафедрой _____ А.В. Родионов

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. 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]
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.
4. 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)
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 с. — 978-5-4383-0161-5. — Режим доступа: http://www.iprbookshop.ru/73641.html
9. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс] / Д.А. Скрипник. — Электрон. текстовые данные. — М. : Интернет-Университет

Информационных Технологий (ИНТУИТ), 2016. — 424 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/52161.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: https://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