

Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Проректор по учебной работе
к.э.н., доцент Измestьев А.А



17.06.2019г.

Рабочая программа дисциплины
Б1.О.14. Информационная безопасность

Направление подготовки: 09.03.03 Прикладная информатика
Направленность (профиль): Информационные системы и технологии в
управлении

Квалификация выпускника: бакалавр

Форма обучения: очная, заочная

	Очная ФО	Заочная ФО
Курс	3	3
Семестр	31	31
Лекции (час)	28	6
Практические (сем, лаб.) занятия (час)	28	10
Самостоятельная работа, включая подготовку к экзаменам и зачетам (час)	52	92
Курсовая работа (час)		
Всего часов	108	108
Зачет (семестр)	31	31
Экзамен (семестр)		

Иркутск 2019

Программа составлена в соответствии с ФГОС ВО по направлению 09.03.03
Прикладная информатика.

Автор М.М. Бусько

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

Заведующий кафедрой С.С. Ованесян

Дата актуализации рабочей программы: 30.06.2020

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 не документированной 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
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ОПК-5	Способен устанавливать программное и аппаратное обеспечение для информационных и автоматизированных систем

Структура компетенции

Компетенция	Формируемые ЗУНы
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с	3. Знать, как решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	У. Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности Н. Владеть навыками решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ОПК-5 Способен установить программное и аппаратное обеспечение для информационных и автоматизированных систем	З. Знать особенности, принципы и технологии инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем У. Уметь устанавливать программное и аппаратное обеспечение для информационных и автоматизированных систем Н. Владеть навыками инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем

3. Место дисциплины (модуля) в структуре образовательной программы

Принадлежность дисциплины - БЛОК 1 ДИСЦИПЛИНЫ (МОДУЛИ):
Обязательная часть.

Предшествующие дисциплины (освоение которых необходимо для успешного освоения данной): "Информационные системы и технологии", "Основы алгоритмизации", "Программирование", "Правоведение", "Организация ЭВМ и систем", "Программная инженерия"

Дисциплины, использующие знания, умения, навыки, полученные при изучении данной: "Проектирование информационных систем", "Блокчейн технологии в экономике", "Информационное право", "Взаимодействие открытых систем", "Разработка распределенных программных систем"

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 3 зач. ед., 108 часов.

Вид учебной работы	Количество часов (очная ФО)	Количество часов (заочная ФО)
Контактная(аудиторная) работа		
Лекции	28	6
Практические (сем, лаб.) занятия	28	10
Самостоятельная работа, включая подготовку к экзаменам и зачетам	52	92
Всего часов	108	108

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	Тема 1. Основы информационной безопасности	31	0	2	14		Практическая работа №1. Идентификация источников антропогенных угроз безопасности информации
2	Тема 2. Правовая защита информации	31	1	2	12		Практическая работа №2. Разработка частной модели угроз организации
3	Тема 3. Организационная защита информации	31	1	2	12		Практическая работа №3. Оценка риска нарушения информационной безопасности
4	Тема 4. Защита информации в компьютерных информационных системах	31	1	2	12		Практическая работа №4. Управление доступом. Домены безопасности
5	Тема 5. Криптографические методы защиты информации	31	1	2	14		Практическая работа №5. Шифрованная файловая система Windows
6	Тема 6. Защита от вредоносного программного обеспечения и спама	31	1	0	14		
7	Тема 7. Инженерно-технические методы защиты информации	31	1	0	14		
	ИТОГО		6	10	92		

Очная форма обучения

№ п/п	Раздел и тема дисциплины	Семестр	Лекции	Семинар Лаборат. Практич.	Самостоят. раб.	В интерактивной форме	Формы текущего контроля успеваемости
1	Тема 1. Основы	31	4	4	8		Практическая

№ п/п	Раздел и тема дисциплины	Семестр	Лекции	Семинар Лаборат. Практич.	Самостоят. раб.	В интерактивной форме	Формы текущего контроля успеваемости
	информационной безопасности						работа №1. Идентификация источников антропогенных угроз безопасности информации
2	Тема 2. Правовая защита информации	31	4	4	6		Практическая работа №2. Разработка частной модели угроз организации
3	Тема 3. Организационная защита информации	31	4	4	6		Практическая работа №3. Оценка риска нарушения информационной безопасности
4	Тема 4. Защита информации в компьютерных информационных системах	31	4	4	8		Практическая работа №4. Управление доступом. Домены безопасности
5	Тема 5. Криптографические методы защиты информации	31	4	4	8		Практическая работа №5. Шифрованная файловая система Windows
6	Тема 6. Защита от вредоносного программного обеспечения и спама	31	4	4	8		Практическая работа №6. Применение электронной подписи
7	Тема 7. Инженерно-технические методы защиты информации	31	4	4	8		Практическая работа №7. Обеспечение безопасности объекта информатизации
	ИТОГО		28	28	52		

5.2. Лекционные занятия, их содержание

№ п/п	Наименование разделов и тем	Содержание
1.1	Лекция 1. Основы информационной безопасности	Понятие информационной безопасности. Актуальность информационной безопасности. Принципы обеспечения информационной безопасности. Структура информационной безопасности.
1.2	Лекция 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	Лекция 3. 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	Лекция 4. Защита информации по режиму доступа	Классификация информации по видам тайны и степеням конфиденциальности. Защита государственной тайны. Защита коммерческой тайны. Защита персональных данных.
3.1	Лекция 5. Организационная защита информации	Организационная защита информации. Зоны ответственности. Локальные нормативные акты в области информационной безопасности. Организация службы безопасности предприятия.
3.2	Лекция 6. Организация конфиденциального документооборота	Гриффы ограничения доступа к документам. Организация конфиденциального документооборота. Стандарты и спецификации в области информационной безопасности.
4.1	Лекция 7. 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	Лекция 8. Безопасность межсетевых обмена данными	Технологии межсетевых экранов. Технологии виртуальных защищенных сетей (VPN). Анализ защищенности и обнаружение атак. Технологии резервного копирования и восстановления данных.
5.1	Лекция 9. Методы криптографического преобразования информации	Классификация методов криптографического закрытия информации. Симметричные криптосистемы. Криптосистемы с открытым ключом.
5.2	Лекция 10. Практическое применение криптографии	Квантовая криптография. Стеганография. Электронная подпись.
6.1	Лекция 11. Вредоносное программное обеспечение	Условия существования вредоносных программ. Классификация вредоносных программ.
6.2	Лекция 12. Защита компьютерных систем от воздействия вредоносных программ	Основы работы антивирусных программ. Защита компьютерных систем от воздействия вредоносных программ. Защита от СПАМА.
7.1	Лекция 13. Инженерно-техническая защита информации	Инженерно-техническая защита информации. Технические каналы утечки информации. Средства выявления каналов утечки информации.
7.2	Лекция 14. Методы и способы защиты	Методы и способы защиты информации от утечки по техническим каналам. Физическая укрепленность объекта

№ п/п	Наименование разделов и тем	Содержание
	информации от утечки по техническим каналам	информатизации.

5.3. Семинарские, практические, лабораторные занятия, их содержание

№ раздела и темы	Содержание и формы проведения
1	Семинар 1. Идентификация источников антропогенных угроз безопасности информации. Выполнение практической работы №1
1	Семинар 2. Идентификация источников антропогенных угроз безопасности информации. Защита отчета по практической работе №1
2	Семинар 3. Разработка частной модели угроз организации. Выполнение практической работы №2
2	Семинар 4. Разработка частной модели угроз организации. Защита отчета по практической работе №2
3	Семинар 5. Оценка риска нарушения информационной безопасности. Выполнение практической работы №3
3	Семинар 6. Оценка риска нарушения информационной безопасности. Защита отчета по практической работе №3
4	Семинар 7. Управление доступом. Домены безопасности. Выполнение практической работы №4
4	Семинар 8. Управление доступом. Домены безопасности. Защита отчета по практической работе №4
5	Семинар 9. Шифрованная файловая система Windows. Выполнение практической работы №5
5	Семинар 10. Шифрованная файловая система Windows. Защита отчета по практической работе №5
6	Семинар 11. Применение электронной подписи. Выполнение практической работы №6
6	Семинар 12. Применение электронной подписи. Защита отчета по практической работе №6
7	Семинар 13. Обеспечение безопасности объекта информатизации. Выполнение практической работы №7
7	Семинар 14. Обеспечение безопасности объекта информатизации. 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.п, У.1...У.п, Н.1...Н.п)	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	ОПК-3	<p>З.Знать, как решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности</p> <p>У.Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности</p> <p>Н.Владеть навыками решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности</p>	Практическая работа №1. Идентификация источников антропогенных угроз безопасности информации	<p>9-10 баллов — сформированные систематические знания; на высоком уровне осуществляемые 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 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)</p>
2	2. Тема 2. Правовая защита информации	ОПК-3	З.Знать, как решать стандартные задачи профессиональной деятельности на основе информационной и	Практическая работа №2. Разработка частной модели угроз организации	14-15 баллов — сформированные систематические знания; на высоком уровне осуществляемые

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1...З.п, У.1...У.п, Н.1...Н.п))	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)
			библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности У. Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности Н. Владеть навыками решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности		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 применения навыков; 7-10 баллов — общие, но не структурированные знания; не систематически осуществляемые умения; не систематически применяемые навыки; 6 и менее баллов — студент обнаружил несостоятельность ответов (15)
3	3. Тема 3. Организационная защита информации	ОПК-3	З. Знать, как решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом	Практическая работа №3. Оценка риска нарушения информационной безопасности	14-15 баллов — сформированные систематические знания; на высоком уровне осуществляемые умения, успешно применяемые навыки; 11-13 баллов — сформированные, но содержащие

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1...З.п, У.1...У.п, Н.1...Н.п)	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)
			основных требований информационной безопасности У. Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности Н. Владеть 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 знания; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее отдельные пробелы применения навыков; 7-10 баллов — общие, но не структурированные знания; не систематически осуществляемые умения; не систематически применяемые навыки; 6 и менее баллов — студент обнаружил несостоятельность ответов (15)
4	4. Тема 4. Защита информации в компьютерных информационных системах	ОПК-5	З. Знать особенности, принципы и технологии инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем У. Уметь инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем	Практическая работа №4. Управление доступом. Домены безопасности	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

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1...З.п, У.1...У.п, Н.1...Н.п)	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)
			Н. Владеть навыками инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем		пробелы умения; 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-5	З. Знать особенности, принципы и технологии инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем У. Уметь инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем Н. Владеть навыками инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем	Практическая работа №5. Шифрованная файловая система Windows	14-15 баллов — сформированные систематические знания; на высоком уровне осуществляе мые 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

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1...З.п, У.1...У.п, Н.1...Н.п)	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)
					структурированные знания; не систематически осуществляемые умения; не систематически применяемые навыки; 6 и менее баллов — студент обнаружил несостоятельность ответов (15)
6	6. Тема 6. Защита от вредоносного программного обеспечения и спама	ОПК-5	З.Знать особенности, принципы и технологии инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем У.Уметь инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем Н.Владеть навыками инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем	Практическая работа №6. Применение электронной подписи	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 систематически применяемые навыки; 6 и менее баллов — студент

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1...З.п, У.1...У.п, Н.1...Н.п))	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)
					обнаружил несостоятельность ответов (15)
7	7. Тема 7. Инженерно-технические методы защиты информации	ОПК-5	<p>З.Знать особенности, принципы и технологии инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем</p> <p>У.Уметь инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем</p> <p>Н.Владеть навыками инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем</p>	Практическая работа №7. Обеспечение безопасности объекта информатизации	<p>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 систематически применяемые навыки; 6 и менее баллов — студент обнаружил несостоятельность ответов (15)</p>
				Итого	100

6.2. Промежуточный контроль (зачет, экзамен)

Рабочим учебным планом предусмотрен Зачет в семестре 31.

ВОПРОСЫ ДЛЯ ПРОВЕРКИ ЗНАНИЙ:

1-й вопрос билета (30 баллов), вид вопроса: Тест/проверка знаний. Критерий: Каждый вопрос теста оценивается в 1 балл.

Компетенция: ОПК-3 Способен 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, как решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

1. Актуальность информационной безопасности.
2. Грифы ограничения доступа к документам.
3. Защита государственной тайны.
4. Защита коммерческой тайны.
5. Защита персональных данных.
6. Локальные нормативные акты в области информационной безопасности.
7. Организационная защита информации. Зоны ответственности.
8. Организация конфиденциального документооборота.
9. Организация службы безопасности предприятия.
10. Понятие информационной безопасности.
11. Правовая защита интересов личности, общества и государства от информационных угроз.
12. Принципы обеспечения информационной безопасности.
13. Структура информационной безопасности.
14. Структура нормативной базы Российской Федерации по вопросам информационной безопасности.
15. Структура системы защиты информации РФ.
16. Угрозы безопасности в информационной сфере.

Компетенция: ОПК-5 Способен устанавливать программное и аппаратное обеспечение для информационных и автоматизированных систем

Знание: Знать особенности, принципы и технологии установки программного и аппаратного обеспечения для информационных и автоматизированных систем

17. Анализ защищенности и обнаружение атак.
18. Анализ угроз информационной безопасности компьютерных систем.
19. Защита компьютерных систем от воздействия вредоносных программ.
20. Защита от СПАМА.
21. Идентификация, аутентификация и управление доступом.
22. Инженерно-техническая защита информации.
23. Квантовая криптография.
24. Классификация вредоносных программ.
25. Классификация информации по видам тайны и степеням конфиденциальности.
26. Классификация методов криптографического закрытия информации.
27. Криптосистемы с открытым ключом.
28. Методы и способы защиты информации от утечки по техническим каналам.
29. Обеспечение безопасности операционных систем.
30. Основы работы антивирусных программ.
31. Симметричные криптосистемы.
32. Средства выявления каналов утечки информации.

33. Стеганография.
34. Технические каналы утечки информации.
35. Технологии виртуальных защищенных сетей (VPN).
36. Технологии защиты информации в компьютерных системах.
37. Технологии межсетевое экранирования.
38. Технологии резервного копирования и восстановления данных.
39. Условия существования вредоносных программ.
40. Физическая укрепленность объекта информатизации.
41. Электронная подпись.

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: ОПК-3 Способен 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 решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Задача № 1. Определите к какому типу по ограничению доступа относится информация, представленная в вашем варианте задания и объясните какие нормативно-правовые документы устанавливают этот статус.

Компетенция: ОПК-5 Способен устанавливать программное и аппаратное обеспечение для информационных и автоматизированных систем

Умение: Уметь устанавливать программное и аппаратное обеспечение для информационных и автоматизированных систем

Задача № 2. Установите правовой статус информации со ссылкой на нормативные документы и определите какие свойства информационной безопасности следует поддерживать.

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: ОПК-3 Способен 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 решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Задание № 1. Для определенного объекта защиты информации необходимо провести анализ его защищенности и определить источники появления угроз.

Компетенция: ОПК-5 Способен устанавливать программное и аппаратное обеспечение для информационных и автоматизированных систем

Навык: Владеть навыками инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем

Задание № 2. Проанализировать объект защиты и классифицировать возможные угрозы по источнику и предложить меры и средства нейтрализации наиболее актуальных.

ОБРАЗЕЦ БИЛЕТА

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

Направление - 09.03.03 Прикладная
информатика
Профиль - Информационные системы и
технологии в управлении
Кафедра математических методов и
цифровых технологий
Дисциплина - Информационная
безопасность

БИЛЕТ № 1

1. Тест (30 баллов).
2. Установите правовой статус информации со ссылкой на нормативные документы и определите какие свойства информационной безопасности следует поддерживать. (35 баллов).
3. Для определенного объекта защиты информации необходимо провести анализ его защищенности и определить источники появления угроз. (35 баллов).

Составитель _____ М.М. Бусько

Заведующий кафедрой _____ С.С. Ованесян

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» \[08.09.2017\]](http://www.iprbookshop.ru/52209.html)
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>](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/> \(30.08.2017\)](http://bdu.fstec.ru/)
4. [Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00. <http://fstec.ru/component/attachments/download/489>](http://fstec.ru/component/attachments/download/489)
5. [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» \[08.09.2017\]](http://www.iprbookshop.ru/61625.html)
6. [Перечень средств защиты информации, сертифицированных ФСБ России. \[http://clsz.fsb.ru/files/download/svedenia_po_sertifikatam_\\(010717\\).doc\]\(http://clsz.fsb.ru/files/download/svedenia_po_sertifikatam_\(010717\).doc\)](http://clsz.fsb.ru/files/download/svedenia_po_sertifikatam_(010717).doc)
7. [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>](http://www.iprbookshop.ru/73641.html)
8. [Скрипник Д.А. Общие вопросы технической защиты информации \[Электронный ресурс\] / Д.А. Скрипник. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий \(ИНТУИТ\), 2016. — 424 с. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/52161.html>](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.grebennikov.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