Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

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

_____

25.06.2021г.

Рабочая программа дисциплины
Б1.Э.2. Защита информации в информационных системах

Направление подготовки: 09.04.03 Прикладная информатика
Направленность (профиль): Цифровые технологии в экономике
Квалификация выпускника: магистр
Форма обучения: очная, заочная

	Очная ФО	Заочная ФО
Курс	1	1
Семестр	11	11
Лекции (час)	28	6
Практические (сем, лаб.) занятия (час)	28	12
Самостоятельная работа, включая подготовку к экзаменам и зачетам (час)	196	234
Курсовая работа (час)		
Всего часов	252	252
Зачет (семестр)		
Экзамен (семестр)	11	11

Иркутск 2021

Программа составлена в соответствии с ФГОС ВО по направлению 09.04.03 Прикладная информатика.

Автор М.М. Бусько

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

Заведующий кафедрой С.С. Ованесян

1. Цели изучения дисциплины

- приобретение знаний о месте и роли защиты информации в общей системе безопасности;
- формирование знаний и умений, связанных с содержанием мероприятий по защите информации;
- освоение направлений правового регулирования в сфере защиты информации, в том числе с учетом международной практики;
- формирование умений формального представления моделей безопасности (управления доступом, целостности и т. д.).
- формирование навыков оценки информационной безопасности и определения информационных рисков.

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
ПК-4	Способен управлять процессами разработки и сопровождения требований к системам и управлению качеством систем
ПК-6	Способен управлять инфраструктурой разработки и сопровождением требований к системам

Структура компетенции

Компетенция	Формируемые ЗУНы
ПК-4 Способен управлять процессами разработки и сопровождения требований к системам и управлению качеством систем	З. Знать теоретические основы управления процессами разработки и сопровождения требований к системам и управлению качеством систем У. Уметь управлять процессами разработки и сопровождения требований к системам и управлению качеством систем Н. Владеть навыками управления процессами разработки и сопровождения требований к системам и управлению качеством систем
ПК-6 Способен управлять инфраструктурой разработки и сопровождением требований к системам	З. Знать теоретические основы управления инфраструктурой разработки и сопровождения требований к системам У. Уметь управлять инфраструктурой разработки и сопровождения требований к системам Н. Владеть навыками управления инфраструктурой разработки и сопровождения требований к системам

3. Место дисциплины (модуля) в структуре образовательной программы

Принадлежность дисциплины - БЛОК 1 ДИСЦИПЛИНЫ (МОДУЛИ): Элективная дисциплина.

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 7 зач. ед.,252 часов.

Вид учебной работы	Количество часов (очная ФО)	Количество часов (заочная ФО)
Контактная(аудиторная) работа		
Лекции	28	6
Практические (сем, лаб.) занятия	28	12
Самостоятельная работа, включая подготовку к экзаменам и зачетам	196	234
Всего часов	252	252

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	Развитие информационного общества и защита информации	11	1		34		
2	Общее содержание мероприятий по защите информации	11	1	2	34		Практическая работа №2
3	Меры и средства обеспечения свойств информационной безопасности	11	1	2	34		Практическая работа №3
4	Правовое регулирование в сфере защиты информации	11	1	2	34		Практическая работа №4
5	Основы формальной теории защиты информации	11	1	2	32		Практическая работа №5
6	Анализ информационных рисков	11	1	2	34		Практическая работа № 6
7	Инструментальные средства анализа информационных рисков	11		2	32		Практическая работа № 7
	ИТОГО		6	12	234		

Очная форма обучения

№ п/п	Раздел и тема дисциплины	Семе-стр	Лек-ции	Семинар Лаборат. Практич.	Само-стоят. раб.	В интера-ктивной форме	Формы текущего контроля успеваемости
1	Развитие информационного общества и защита информации	11	4	4	28		Практическая работа №1
2	Общее содержание мероприятий по защите информации	11	4	4	28		Практическая работа №2
3	Меры и средства обеспечения свойств информационной безопасности	11	4	4	28		Практическая работа №3
4	Правовое регулирование в сфере защиты информации	11	4	4	28		Практическая работа №4
5	Основы формальной теории защиты информации	11	4	4	28		Практическая работа №5
6	Анализ информационных рисков	11	4	4	28		Практическая работа № 6
7	Инструментальные средства анализа информационных рисков	11	4	4	28		Практическая работа № 7
	ИТОГО		28	28	196		

5.2. Лекционные занятия, их содержание

№ п/п	Наименование разделов и тем	Содержание
1.1	Развитие информационного общества и защита информации	Проблемы развития теории и практики обеспечения информационной безопасности. Основные понятия и определения в области информационной безопасности. Термины, определяющие научную основу информационной безопасности. Термины, определяющие предметную основу информационной безопасности. Термины, определяющие характер деятельности по обеспечению информационной безопасности. Определение информационной безопасности в свете информационных проблем современного общества.
1.2	Развитие информационного общества и информационная безопасность	Основные составляющие информационной безопасности. Значение информационной безопасности для субъектов информационных отношений. Составляющие национальных интересов Российской Федерации в информационной сфере. Стратегия национальной безопасности Российской Федерации до 2020 года. Доктрина информационной безопасности Российской Федерации. Международное сотрудничество в области информационной безопасности: проблемы и перспективы.
2.1	Общее содержание	Понятие и сущность защиты информации. Цели защиты

№ п/п	Наименование разделов и тем	Содержание
	мероприятий по защите информации	информации. Концептуальная модель информационной безопасности. Предмет защиты информации. Информация как объект права собственности. Объект защиты информации. Угрозы информационной безопасности: случайные и преднамеренные. Модель гипотетического нарушителя информационной безопасности.
2.2	Общее содержание мероприятий по защите информации	Системное обеспечение защиты информации. Основные принципы построения системы защиты. Методы защиты информации. Построение систем защиты от угроз нарушения конфиденциальности информации. Модель системы защиты. Организационные меры и меры обеспечения физической безопасности.
3.1	Меры и средства обеспечения свойств информационной безопасности	Идентификация и аутентификация. Разграничение доступа. Криптографические методы обеспечения конфиденциальности информации. Методы защиты внешнего периметра. Протоколирование и аудит. Построение систем защиты от угроз нарушения целостности. Принципы обеспечения целостности. Криптографические методы обеспечения целостности информации.
3.2	Меры и средства обеспечения свойств информационной безопасности	Построение систем защиты от угроз нарушения доступности. Минимизация ущерба от аварий и стихийных бедствий. Повышение надежности информационной системы. Создание отказоустойчивых информационных систем. Оптимизация взаимодействия пользователей и обслуживающего персонала. Модели защиты информации.
4.1	Правовое регулирование в сфере защиты информации	Информация как объект преступных посягательств. Система правоохранительных органов РФ, связанных с информационной сферой. Понятие компьютерных преступлений и их классификация. Субъект преступлений в сфере компьютерной информации: особенности. Преступления, совершенные с помощью компьютера и их особенности.
4.2	Правовое регулирование в сфере защиты информации	Основы расследования компьютерных преступлений. Доказательства и доказывание. Международное право при компьютерных инцидентах. Нормы уголовного права некоторых зарубежных стран. Правовые документы по информационной безопасности. Технические документы по информационной безопасности.
5.1	Основы формальной теории защиты информации	Основные определения. Монитор безопасности обращений. Формальные модели управления доступом. Модель Харрисона-Руззо-Ульмана. Модель Белла-ЛаПадулы. Формальные модели целостности.
5.2	Основы формальной теории защиты информации	Модель Кларка-Вилсона. Модель Биба. Совместное использование моделей безопасности. Ролевое управление доступом. Скрытые каналы передачи информации.
6.1	Анализ информационных рисков	Основные цели и задачи аудита безопасности и анализа рисков. Актуальность аудита безопасности и анализа рисков. Оценка уровня безопасности компьютерных информационных систем. Возможные виды аудита безопасности компьютерных информационных систем. Возможные методики аудита

№ п/п	Наименование разделов и тем	Содержание
		безопасности компьютерных информационных систем. Возможные алгоритмы аудита безопасности компьютерных информационных систем. Анализ информационных рисков. Методы оценивания информационных рисков. Роль анализа рисков в процессе создания корпоративной системы информационной безопасности (на примере модели LifeCycle Security). Возможная методика реорганизации корпоративной системы безопасности. Проектирование системы обеспечения безопасности объекта.
6.2	Анализ информационных рисков	Аналитический обзор инструментальных средств для анализа рисков и защищенности корпоративных систем Intranet/Internet. Инструментальные проверки уровня безопасности. Internet Scanner и System Security Scanner. Сканер уязвимости Symantec NetRecon. Система централизованного управления безопасностью Enterprise Security Manager. Сканер уязвимости системы безопасности Cisco Secure Scanner (NetSonar). Сканер Retina. Сканер Xspider. Пример использования средств активного аудита. Инструментальные средства анализа рисков. Количественный подход к анализу рисков на примере RiskWatch. Выбор оптимальной стратегии защиты компании.
7.1	Инструментальные средства анализа информационных рисков	Аналитический обзор инструментальных средств для анализа рисков и защищенности корпоративных систем Intranet/Internet. Инструментальные проверки уровня безопасности. Internet Scanner и System Security Scanner. Сканер уязвимости Symantec NetRecon. Система централизованного управления безопасностью Enterprise Security Manager.
7.2	Инструментальные средства анализа информационных рисков	Сканер уязвимости системы безопасности Cisco Secure Scanner (NetSonar). Сканер Retina. Сканер Xspider. Пример использования средств активного аудита. Инструментальные средства анализа рисков. Количественный подход к анализу рисков на примере RiskWatch. Выбор оптимальной стратегии защиты компании.

5.3. Семинарские, практические, лабораторные занятия, их содержание

№ раздела и темы	Содержание и формы проведения
1	Исследование математических методов анализа стойкости парольных систем. Выполнение практической работы №1.
1	Исследование математических методов анализа стойкости парольных систем. Защита отчета по практической работе №1, ответы на контрольные вопросы.
2	Управление доступом. Домены безопасности. Модель распространения прав доступа. Выполнение практической работы №2
2	Управление доступом. Домены безопасности. Модель распространения прав доступа. Защита отчета по практической работе №2, ответы на контрольные вопросы.

№ раздела и темы	Содержание и формы проведения
3	Управление доступом. Реализация мандатной модели политики безопасности. Выполнение практической работы №3
3	Управление доступом. Реализация мандатной модели политики безопасности. Защита отчета по практической работе №3, ответы на контрольные вопросы.
4	Модель ролевого доступа при иерархически организованной системе ролей. Выполнение практической работы №4
4	Модель ролевого доступа при иерархически организованной системе ролей. Защита отчета по практической работе №4, ответы на контрольные вопросы.
5	Применение теории графов для моделирования систем защиты информации. Выполнение практической работы №5
5	Применение теории графов для моделирования систем защиты информации. Защита отчета по практической работе №5, ответы на контрольные вопросы.
6	Менеджмент риска информационной безопасности в соответствии с ГОСТ Р ИСО/МЭК 27005-2010. Выполнение практической работы №6
6	Менеджмент риска информационной безопасности в соответствии с ГОСТ Р ИСО/МЭК 27005-2010. Защита отчета по практической работе №6, ответы на контрольные вопросы.
7	Определение оценки вероятности реализации угроз. Выполнение практической работы №7
7	Определение оценки вероятности реализации угроз. Защита отчета по практической работе №7, ответы на контрольные вопросы.

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. Развитие информационного общества и защита информации	ПК-4	З.Знать теоретические основы управления процессами разработки и сопровождения требований к системам и управлению качеством систем У.Уметь управлять процессами разработки и сопровождения требований к системам и	Практическая работа №1	14-15 — сформированные систематические знания; на высоком уровне осуществляемые умения, успешно применяемые навыки. 11-13 баллов — сформированные, но содержащие отдельные пробелы знания; в целом

№ 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)
			управлению качеством систем Н.Владеть навыками управления процессами разработки и сопровождения требований к системам и управлению качеством систем		успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее отдельные пробелы применение навыков. 6-10 баллов — общие, но не структурированные знания; не систематически осуществляемые умения; не систематически применяемые навыки. 5 и менее баллов — студент обнаружил несостоятельность ответов (15)
2	2. Общее содержание мероприятий по защите информации	ПК-4	З.Знать теоретические основы управления процессами разработки и сопровождения требований к системам и управлению качеством систем У.Уметь управлять процессами разработки и сопровождения требований к системам и управлению качеством систем Н.Владеть навыками управления процессами разработки и сопровождения требований к системам и управлению качеством систем	Практическая работа №2	14-15 — 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. 6-10

№ 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)
					баллов — общие, но не структурированные знания; не систематически осуществляемые умения; не систематически применяемые навыки. 5 и менее баллов — студент обнаружил несостоятельность ответов (15)
3	3. Меры и средства обеспечения свойств информационной безопасности	ПК-4	З.Знать теоретические основы управления процессами разработки и сопровождения требований к системам и управлению качеством систем У.Уметь управлять процессами разработки и сопровождения требований к системам и управлению качеством систем Н.Владеть навыками управления процессами разработки и сопровождения требований к системам и управлению качеством систем	Практическая работа №3	14-15 — 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. 6-10 баллов — общие, но не структурированные знания; не систематически осуществляемые умения; не систематически применяемые навыки. 5 и менее баллов —

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1…З.n, У.1…У.n, Н.1…Н.n)	Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы (Наименование оценочного средства)	Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (по 100-балльной шкале)
					студент обнаружил несостоятельность ответов (15)
4	4. Правовое регулирование в сфере защиты информации	ПК-6	З.Знать теоретические основы управления инфраструктурой разработки и сопровождения требований к системам У.Уметь управлять инфраструктурой разработки и сопровождения требований к системам Н.Владеть навыками управления инфраструктурой разработки и сопровождения требований к системам	Практическая работа №4	14-15 — 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. 6-10 баллов — общие, но не структурированные знания; не систематически осуществляемые умения; не систематически применяемые навыки. 5 и менее баллов — студент обнаружил несостоятельность ответов (15)
5	5. Основы формальной теории защиты информации	ПК-6	З.Знать теоретические основы управления инфраструктурой разработки и сопровождения требований к системам	Практическая работа №5	14-15 — сформированные систематические знания; на высоком уровне осуществляемые умения, успешно

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1…З.n, У.1…У.n, Н.1…Н.n)	Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы (Наименование оценочного средства)	Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (по 100-балльной шкале)
			У.Уметь управлять инфраструктурой разработки и сопровождения требований к системам Н.Владеть навыками управления инфраструктурой разработки и сопровождения требований к системам		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. 6-10 баллов — общие, но не структурированные знания; не систематически осуществляемые умения; не систематически применяемые навыки. 5 и менее баллов — студент обнаружил несостоятельность ответов (15)
6	6. Анализ информационных рисков	ПК-6	З.Знать теоретические основы управления инфраструктурой разработки и сопровождения требований к системам У.Уметь управлять инфраструктурой разработки и сопровождения требований к системам Н.Владеть навыками управления инфраструктурой разработки и сопровождения	Практическая работа № 6	14-15 — 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.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)
			требований к системам		пробелы умения; в целом успешное, но содержащее отдельные пробелы применение навыков. 6-10 баллов — общие, но не структурированные знания; не систематически осуществляемые умения; не систематически применяемые навыки. 5 и менее баллов — студент обнаружил несостоятельность ответов (15)
7	7. Инструментальные средства анализа информационных рисков	ПК-6	З.Знать теоретические основы управления инфраструктурой разработки и сопровождения требований к системам У.Уметь управлять инфраструктурой разработки и сопровождения требований к системам Н.Владеть навыками управления инфраструктурой разработки и сопровождения требований к системам	Практическая работа № 7	9-10 — 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. 4-6 баллов — общие, но не структурированн

№ 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)
					ые знания; не систематически осуществляемые умения; не систематически применяемые навыки. 4 и менее баллов — студент обнаружил несостоятельность ответов (10)
				Итого	**100**

6.2. Промежуточный контроль (зачет, экзамен)

Рабочим учебным планом предусмотрен Экзамен в семестре 11.

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: ПК-4 Способен управлять процессами разработки и сопровождения требований к системам и управлению качеством систем

Знание: Знать теоретические основы управления процессами разработки и сопровождения требований к системам и управлению качеством систем

1. Аудит информационной безопасности.
2. Направления работ по защите информации.
3. Основные понятия и определения в области информационной безопасности.
4. Оценка риска нарушения информационной безопасности.
5. Проблемы развития теории и практики обеспечения информационной безопасности.
6. Система защиты от угроз нарушения доступности информации.
7. Система защиты от угроз нарушения конфиденциальности информации.
8. Система защиты от угроз нарушения целостности информации.
9. Требования к защите информации в автоматизированных системах.
10. Угрозы информационной безопасности, источники угроз, потенциал нарушителя.
11. Управление информационной безопасностью.

Компетенция: ПК-6 Способен управлять инфраструктурой разработки и сопровождением требований к системам

Знание: Знать теоретические основы управления инфраструктурой разработки и сопровождения требований к системам

12. Дискреционная модель Кларка-Вильсона.
13. Дискреционное управление доступом.
14. Идентификация и аутентификация.
15. Криптографические методы обеспечения конфиденциальности информации.
16. Мандатная модель Кена Биба.
17. Мандатное управление доступом.
18. Методы анализа и оценки защищенности компьютерных систем.
19. Модели дискреционного доступа на основе матрицы доступа.
20. Модель TAKE-GRANT.
21. Модель Белла-ЛаПадулы.
22. Монитор безопасности обращений.
23. Ролевое разграничение доступа.
24. Скрытые каналы передачи информации.
25. Субъектно-объектная модель компьютерной системы.
26. Тематическое разграничение доступа.
27. Управление доступом.
28. Формальная модель управления доступом Харрисона-Руззо-Ульмана.
29. Формальные модели обеспечения целостности данных.

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: ПК-4 Способен управлять процессами разработки и сопровождения требований к системам и управлению качеством систем

Умение: Уметь управлять процессами разработки и сопровождения требований к системам и управлению качеством систем

Задача № 1. Задать критерии безопасности по обеспечению целостности информации при мандатном управлении доступом.

Задача № 2. Обосновать и составить систему уровней допусков пользователей, грифов секретности объектов доступа и матрицу доступа для мандатного управления доступом.

Задача № 3. Определить набор прав субъекта (пользователя) по отношению к объекту в соответствии с решеткой безопасности мандатного управления доступом.

Задача № 4. Определить направления потоков информации между субъектами и объектами доступа при выполнении операций с файлами.

Задача № 5. Построить матрицу доступа по заданным параметрам при дискреционном управлении доступом.

Задача № 6. Построить систему иерархически организованных ролей с наследованием прав «сверху».

Задача № 7. Построить систему иерархически организованных ролей с наследованием прав «снизу».
Задача № 8. Построить систему команд перехода передачи субъекту x прав доступа a на объект s от субъекта y в соответствии с моделью Take-Grant.
Задача № 9. Построить сценарий утечки прав доступа субъекта к объекту при дискреционном управлении доступа.
Задача № 10. Привести пример реализации скрытого по времени канала передачи информации.
Задача № 11. Привести пример реализации скрытого по памяти канала передачи информации.

Компетенция: ПК-6 Способен управлять инфраструктурой разработки и сопровождением требований к системам

Умение: Уметь управлять инфраструктурой разработки и сопровождения требований к системам
Задача № 12. В каком документе изложены требования, предъявляемые к межсетевым экранам, выполнение которых необходимо для успешного прохождения аттестации АС?
Задача № 13. В системе защиты аттестуемой по требованиям СТР-К АС требуется использование сертифицированного средства антивирусной защиты. Выполнение требований какого документа должен подтверждать сертификат на антивирусное средство?
Задача № 14. В системе защиты аттестуемой по требованиям СТР-К АС требуется использование сертифицированного средства защиты от НСД. Выполнение требований какого документа должен подтверждать сертификат на средство защиты?
Задача № 15. В системе защиты аттестуемой по требованиям СТР-К АС требуется использование сертифицированного средства криптографической защиты информации. Выполнение требований какого документа должен подтверждать сертификат на средство защиты?
Задача № 16. ИТ-компания занимается проектированием средств и систем информатизации в защищенном исполнении. Нужно ли в связи с этим получать какую-нибудь лицензию? Если нужно, то какую?
Задача № 17. Крупная строительная организация содержит базу персональных данных более 100000 субъектов персональных данных. Нужно ли в связи с этим получать какую-нибудь лицензию? Если нужно, то какую? Какие еще обязательные действия должна предпринять организация?
Задача № 18. Определить уровень проектной защищенности информационной системы по заданным функционально-структурным характеристикам и условиям эксплуатации.
Задача № 19. Организация приняла решение ввести режим коммерческой тайны. Нужно ли в связи с этим получать какую-нибудь лицензию? Если нужно, то какую?
Задача № 20. Организация приняла решение заниматься предоставлением услуг удостоверяющего центра. Нужно ли в связи с этим получать какую-нибудь лицензию? Если нужно, то какую? Какие еще обязательные действия должна предпринять организация?
Задача № 21. Почему для построения системы защиты, аттестуемой по требованиям СТР-К АС выбирают именно сертифицированные средства защиты?
Задача № 22. Предложить вариант системы двухуровневой аутентификации на основе «знания чего-либо».
Задача № 23. Предложить вариант системы двухуровневой аутентификации на основе неотъемлемых характеристик субъекта.
Задача № 24. Предложить вариант системы двухуровневой аутентификации на основе программно-аппаратных носителей ключевой информации (на основе «обладания чем-либо»).

Задача № 25. Предложить шкалу качественных оценок ущерба при нарушении конфиденциальности персональных данных с позиции оператора и с позиции субъекта персональных данных.
Задача № 26. Предложить шкалу качественных оценок ущерба при нарушении целостности персональных данных с позиции оператора и с позиции субъекта персональных данных.
Задача № 27. Федеральное казначейство организует работы по проведению аттестации АС своими силами в своих территориальных подразделениях. Нужна ли лицензия на техническую защиту конфиденциальной информации?
Задача № 28. Что такое «Автоматизированная система»? В чем отличие от понятия «Средство вычислительной техники».
Задача № 29. Что такое «Объект информатизации»? В чем отличие от понятия «Автоматизированная система».

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: ПК-4 Способен управлять процессами разработки и сопровождения требований к системам и управлению качеством систем
Навык: Владеть навыками управления процессами разработки и сопровождения требований к системам и управлению качеством систем
Задание № 1. Для заданного перечня конфиденциальной информации определить информационную среду, в отношении которой реализация угроз приводит к нарушению конфиденциальности, целостности или доступности информации.
Задание № 2. На примере из 3 субъектов доступа (S) и 5 объектов доступа (O) составить матрицу доступа согласно модели Харрисона-Руззо-Ульмана.
Задание № 3. На примере из 3 субъектов доступа и 4 объектов доступа составить диаграмму информационных потоков в соответствии с моделью Белла-ЛаПадулы.
Задание № 4. Описать права доступа субъектов к объектам в системе реализующий дискреционное разграничение доступа с помощью матрицы. Используя элементарные операции (добавление субъекту s права, удаление у субъекта s права, создание нового субъекта s, удаление существующего субъекта s, создание нового объекта o, удаление существующего объекта o) проанализировать состояние защищенности системы.
Задание № 5. Определить тип угроз информационной системе в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных» (утв. Постановлением Правительства РФ от 01.11.2012 N 1119). Исходные данные задаются преподавателем.

Задание № 6. Показать на примере из 3 субъектов доступа и 4 объектов доступа, как матрицу доступа модели Харрисона-Руззо-Ульмана представить в виде системы Белла-ЛаПадулы.
Задание № 7. Построить модель внешнего нарушителя, реализующего несанкционированный доступ в информационной системе персональных данных.
Задание № 8. Построить модель угроз безопасности персональных данных, обрабатываемых в автоматизированных рабочих местах, не имеющих подключения к сетям связи общего пользования и (или) сетям международного информационного обмена.
Задание № 9. Построить модель угроз безопасности персональных данных, обрабатываемых в локальных информационных системах персональных данных, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.
Задание № 10. Построить модель угроз безопасности персональных данных, обрабатываемых в распределенных информационных системах персональных данных, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.
Задание № 11. Составить базовую модель внутреннего нарушителя информационной безопасности в отношении коммерческой тайны.

Компетенция: ПК-6 Способен управлять инфраструктурой разработки и сопровождением требований к системам

Навык: Владеть навыками управления инфраструктурой разработки и сопровождения требований к системам
Задание № 12. Определить актуальность угрозы с высокой возможностью реализации для ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъекты ПДн.
Задание № 13. Определить базовые требования к показателям защищенности средств вычислительной техники 4-го класса.
Задание № 14. Определить возможность реализации угрозы безопасности информации нарушителем с низким потенциалом в отношении системы с высоким уровнем защищенности.
Задание № 15. Определить класс защищенности информационной системы в соответствии с «Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (приказ ФСТЭК № 17 от 11.02.2013). Исходные данные задаются преподавателем.
Задание № 16. Определить необходимый уровень защищенности персональных данных в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных» (утв. Постановлением Правительства РФ от 01.11.2012 N 1119). Исходные данные задаются преподавателем.
Задание № 17. Определить операционные системы, соответствующие требованиям 4 класса защищенности средств вычислительной техники (РД СВТ) и имеющие 3 уровень отсутствия недекларированных возможностей (РД НДВ).
Задание № 18. Определить состав и содержание организационных и технических мер для обеспечения 1 и 2 уровней защищенности персональных данных при их обработке в информационных системах персональных данных.
Задание № 19. Определить состав и содержание организационных и технических мер для обеспечения 3 уровня защищенности персональных данных при их обработке в информационных системах персональных данных.
Задание № 20. Определить состав и содержание организационных и технических мер для обеспечения 4 уровня защищенности персональных данных при их обработке в информационных системах персональных данных.

Задание № 21. Определить степень ущерба, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств.
Задание № 22. Определить степень ущерба, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций.
Задание № 23. Определить требования к реализации защиты информационной системы, ее средств и систем связи и передачи данных с использованием разделения функциональных возможностей по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации (функций безопасности) и функциональных возможностей пользователей по обработке информации.
Задание № 24. Определить требования к реализации защиты машинных носителей информации организацией контроля перемещения используемых в информационной системе машинных носителей информации за пределы контролируемой зоны.
Задание № 25. Определить требования по защите информации от несанкционированного доступа к автоматизированным системам класса защищенности 1А.
Задание № 26. Определить требования по защите информации от несанкционированного доступа к автоматизированным системам класса защищенности 4А.
Задание № 27. Определить уровень возможностей (потенциал) нарушителя, который является внешним субъектом (физическим лицом), обеспечивающим функционирование информационных систем или обслуживающим инфраструктуру оператора.
Задание № 28. Оценить возможности по реализации угроз безопасности информации внешних нарушителей, не имеющих права доступа к информационной системе, ее отдельным компонентам и реализующих угрозы безопасности информации из-за границ информационной системы.
Задание № 29. Оценить возможности по реализации угроз безопасности информации внутренних нарушителей, имеющих право постоянного или разового доступа к информационной системе, ее отдельным компонентам.

ОБРАЗЕЦ БИЛЕТА

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

Направление - 09.04.03 Прикладная информатика
Профиль - Цифровые технологии в экономике
Кафедра математических методов и цифровых технологий
Дисциплина - Защита информации в информационных системах

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Тест (30 баллов).
2. Определить направления потоков информации между субъектами и объектами доступа при выполнении операций с файлами. (35 баллов).
3. Определить требования по защите информации от несанкционированного доступа к автоматизированным системам класса защищенности 1А. (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]
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. 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)
2. Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00. http://fstec.ru/component/attachments/download/489
3. 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]
4. Перечень средств защиты информации, сертифицированных ФСБ России. http://clsz.fsb.ru/files/download/svedenia_po_sertifikatam_(010717).doc
5. 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
6. 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

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

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

Изучать дисциплину рекомендуется в соответствии с той последовательностью, которая обозначена в ее содержании. Для успешного освоения курса обучающиеся должны иметь первоначальные знания базовой части основной образовательной программы подготовки бакалавриата по направлению «Прикладная информатика».

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:
– Гарант платформа F1 7.08.0.163 - информационная справочная система,
– КонсультантПлюс: Версия Проф - информационная справочная система,
– MS Office,

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