МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Лесосибирский филиал федерального государственного бюджетного
образовательного учреждения высшего образования
«Сибирский государственный университет науки и технологий
имени академика М.Ф. Решетнева»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ЗАЩИТА ИНФОРМАЦИИ

Направление подготовки
09.03.01 Информатика и вычислительная техника

Направленность (профиль) образовательной программы
Программное обеспечение средств вычислительной техники и автоматизированных систем

Уровень высшего образования
бакалавриат

Форма обучения
очная, очно-заочная, заочная

Красноярск 2021

Рабочая программа дисциплины составлена в соответствии с актуализированным федеральным государственным образовательным стандартом высшего образования – бакалавриат по направлению подготовки 09.03.01 Информатика и вычислительная техника, утвержденным приказом Министерства науки и высшего образования Российской Федерации 19.09.2017г. №929

Разработчики рабочей программы дисциплины:

Доцент кафедры информационных и технических систем	_____	В.В. Фирер
должность, учёная степень, учёное звание	подпись	И.О. Фамилия
Руководитель ОПОП, к.т.н., доцент, заведующий кафедрой информационных и технических систем	_____	П.А. Егармин
должность, учёная степень, учёное звание	подпись	И.О. Фамилия

Рабочая программа дисциплины рассмотрена на заседании кафедры информационных и технических систем от «09» июня 2021г. протокол № 7

Заведующий кафедрой, к.т.н., доцент	_____	П.А. Егармин
должность, учёная степень, учёное звание	подпись	И.О. Фамилия

Рабочая программа дисциплины рассмотрена на заседании научно-методического совета филиала от «09» июня 2021 г., протокол № 3

Председатель НМС филиала, к.т.н., доцент	_____	С.В. Соболев
должность, учёная степень, учёное звание	подпись	И.О. Фамилия

Рабочая программа дисциплины утверждена в составе ОПОП решением Ученого совета СибГУ им. М.Ф. Решетнева №1 от 25.06.2021г.

АННОТАЦИЯ
Рабочей программы дисциплины
Защита информации

(наименование дисциплины)

Направление подготовки (Специальность)	09.03.01 Информатика и вычислительная техника
Направленность (профиль)	Программное обеспечение средств вычислительной техники и автоматизированных систем

Объем дисциплины составляет 3 зачетные единицы, 108 часов.

Цель и задачи изучения дисциплины

Цель изучения дисциплины	– ознакомление студентов с организационными, техническими, алгоритмическими методами и средствами защиты компьютерной информации, с законодательством и стандартами в области защиты информации, с современными криптосистемами.
Задачи изучения дисциплины:	– изучение проблем защиты информации; – изучение основ криптографии, криптографических алгоритмов, алгоритмов аутентификации, методов и средств сетевой защиты, методов и средств организации защищенных каналов передачи данных, методов и средств обнаружения атак на информационные системы; – получение практических навыков решения типовых задач по обеспечению информационной безопасности.

Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в программе индикаторами достижения компетенций

Код компе-тенции	Содержание компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине, соотнесенные с установленными в программе индикаторами достижения компетенции
ПК-6	Способен к проведению регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы	**ПК-6.1.** Выполняет регламентные работы по поддержке операционных систем сетевых устройств инфокоммуникационной системы **ПК-6.2.** Восстанавливает параметры программного обеспечения сетевых устройств **ПК-6.3.** Выполняет настройку сетевой инфокоммуникационной системы с точки зрения информационной безопасности	**Знать**: – общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети; – инструкции по установке и эксплуатации администрируемых сетевых устройств и программного обеспечения; – протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем **Уметь**: – использовать типовые процедуры восстановления данных; – работать с серверами архивирования и средствами управления операционных систем **Владеть**: – способами восстановления параметров при помощи средств управления специализированных операционных систем сетевого оборудования; – способами оценки эффективности конфигурации сетевых устройств с точки зрения производительности сети и защиты от несанкционированного доступа

Место дисциплины в структуре ОПОП

Дисциплина «Защита информации» (Б1.В.10) входит в часть, формируемую участниками образовательных отношений, блока Б1 «Дисциплины (модули)».

Краткое содержание дисциплины

Раздел 1. Основы информационной безопасности.

Раздел 2. Меры обеспечения защиты информации.

Раздел 3. Информационная безопасность предприятия.

Форма промежуточной аттестации

Зачет.

Оглавление

1. Цель и задачи изучения дисциплины

Цель изучения дисциплины	– ознакомление студентов с организационными, техническими, алгоритмическими методами и средствами защиты компьютерной информации, с законодательством и стандартами в области защиты информации, с современными криптосистемами.
Задачи изучения дисциплины:	– изучение проблем защиты информации; – изучение основ криптографии, криптографических алгоритмов, алгоритмов аутентификации, методов и средств сетевой защиты, методов и средств организации защищенных каналов передачи данных, методов и средств обнаружения атак на информационные системы; – получение практических навыков решения типовых задач по обеспечению информационной безопасности.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в программе индикаторами достижения компетенций

Код компе-тенции	Содержание компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине, соотнесенные с установленными в программе индикаторами достижения компетенции
ПК-6	Способен к проведению регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы	**ПК-6.1.** Выполняет регламентные работы по поддержке операционных систем сетевых устройств инфокоммуникационной системы **ПК-6.2.** Восстанавливает параметры программного обеспечения сетевых устройств **ПК-6.3.** Выполняет настройку сетевой инфокоммуникационной системы с точки зрения информационной безопасности	**Знать**: – общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети; – инструкции по установке и эксплуатации администрируемых сетевых устройств и программного обеспечения; – протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем **Уметь**: – использовать типовые процедуры восстановления данных; – работать с серверами архивирования и средствами управления операционных систем **Владеть**: – способами восстановления параметров при помощи средств управления специализированных операционных систем сетевого оборудования; – способами оценки эффективности конфигурации сетевых устройств с точки зрения производительности сети и защиты от несанкционированного доступа

3. Место дисциплины в структуре ОПОП

Дисциплина «Защита информации» (Б1.В.10) входит в часть, формируемую участниками образовательных отношений, блока Б1 «Дисциплины (модули)».

Изучение курса связано с дисциплинами: «Информатика», «Математика», «Программирование», «Объектно-ориентированное программирование и проектирование», «Сети и телекоммуникации».

Знания, умения и навыки, полученные в ходе изучения дисциплины, являются

необходимыми для изучения дисциплин: «Технология разработки программного обеспечения», «Тестирование и отладка программного обеспечения», «Основы Web-технологий», «Операционные системы», а также для прохождения производственной практики и написания выпускной квалификационной работы.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов.

а) очная форма

Вид учебной работы / номер семестра в УП	Всего, зачетных единиц (акад. часов)	Семестр
Номер семестра		6
Общая трудоемкость дисциплины	**3 (108)**	**3 (108)**
Контактная работа с преподавателем:	**1,5 (54)**	**1,5 (54)**
занятия лекционного типа	0,5 (18)	0,5 (18)
занятия семинарского типа	1 (36)	1 (36)
в том числе: семинары		
практические занятия		
практикумы		
лабораторные работы	1 (36)	1 (36)
коллоквиумы		
иные аналогичные занятия		
в том числе: курсовое проектирование		
групповые консультации		
индивидуальная работа с преподавателем		
иная контактная внеаудиторная работа		
Самостоятельная работа обучающихся:	**1,5 (54)**	**1,5 (54)**
изучение теоретического курса (ТО)	1,5 (54)	1,5 (54)
индивидуальные задания (ИЗ)		
расчетно-графические работы (РГР)		
реферат, эссе (Р)		
курсовое проектирование (КР/КП)		
контрольные работы (Кн.р)		
другие виды самостоятельной работы		
Форма промежуточной аттестации (зачет, зачет с оценкой, экзамен, курсовой проект, курсовая работа)	**зачет**	**зачет**

б) заочная форма

Вид учебной работы / номер семестра в УП	Всего, зачетных единиц (акад. часов)	Семестр	Семестр
Номер семестра		7	8
Общая трудоемкость дисциплины	**3 (108)**	**1 (36)**	**2 (72)**
Контактная работа с преподавателем:	**0,33 (12)**	**0,05 (2)**	**0,28 (10)**
занятия лекционного типа	0,11 (4)	0,05 (2)	0,06 (2)
занятия семинарского типа	0,22 (8)		0,22 (8)
в том числе: семинары			
практические занятия			
практикумы			
лабораторные работы	0,22 (8)		0,22 (8)
коллоквиумы			
иные аналогичные занятия			
в том числе: курсовое проектирование			
групповые консультации			
индивидуальная работа с преподавателем			
иная контактная внеаудиторная работа			
Самостоятельная работа обучающихся:	**2,67 (96)**	**0,95 (34)**	**1,72 (62)**
изучение теоретического курса (ТО)	2,67 (96)	0,95 (34)	1,72 (62)
индивидуальные задания (ИЗ)			
расчетно-графические работы (РГР)			
реферат, эссе (Р)			
курсовое проектирование (КР/КП)			
контрольные работы (Кн.р)			
другие виды самостоятельной работы			
Форма промежуточной аттестации (зачет, зачет с оценкой, экзамен, курсовой проект, курсовая работа)	**зачет**		**зачет**

в) очно-заочная форма

Вид учебной работы / номер семестра в УП	Всего, зачетных единиц (акад. часов)	Семестр
Номер семестра		7
Общая трудоемкость дисциплины	**3 (108)**	**3 (108)**
Контактная работа с преподавателем:	**1,5 (54)**	**1,5 (54)**
занятия лекционного типа	0,5 (18)	0,5 (18)
занятия семинарского типа	1 (36)	1 (36)
в том числе: семинары		
практические занятия		
практикумы		
лабораторные работы	1 (36)	1 (36)
коллоквиумы		
иные аналогичные занятия		
в том числе: курсовое проектирование		
групповые консультации		
индивидуальная работа с преподавателем		
иная контактная внеаудиторная работа		
Самостоятельная работа обучающихся:	**2,5 (90)**	**2,5 (90)**
изучение теоретического курса (ТО)	2,5 (90)	2,5 (90)
индивидуальные задания (ИЗ)		
расчетно-графические работы (РГР)		
реферат, эссе (Р)		
курсовое проектирование (КР/КП)		
контрольные работы (Кн.р)		
другие виды самостоятельной работы		
Форма промежуточной аттестации (зачет, зачет с оценкой, экзамен, курсовой проект, курсовая работа)	**зачет**	**зачет**

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

а) очная форма

№ п/п	Раздел/тема	Занятия лекционного типа, (акад. часов)	Занятия семинарского типа, (акад. часов)		Самостоятельная работа, (акад. часов)	Формируемые компетенции
			Семинары и/или практические занятия	Лабораторные работы		
1	Раздел 1. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ					ПК–6
1.1	Основы информационной безопасности	2			4	
1.2	Политика государства в области информационной безопасности	2		6	2	
1.3	Угрозы, нарушители и модель угроз безопасности информации	2		4	4	
2	Раздел 2. МЕРЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ					ПК–6
2.1	Организационные меры защиты информации	2		4	4	
2.2	Криптографические меры защиты информации	2		10	2	
2.3	Программно-технические меры защиты информации	2		6	4	
2.4	Стеганографическая и техническая защита информации	2		6	4	
3	Раздел 3. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ					ПК–6
3.1	Политика безопасности предприятия	2			10	
3.2	Системы обнаружения и предотвращения компьютерных атак	1			10	
3.3	Основные стандарты в области информационной безопасности	1			10	
	Итого в семестр:	**18**		**36**	**54**	
	Всего:	**18**		**36**	**54**	

б) заочная форма

№ п/п	Раздел/тема	Занятия лекционного типа, (акад. часов)	Занятия семинарского типа, (акад. часов)		Самостоятельная работа, (акад. часов)	Формируемые компетенции
			Семинары и/или практические занятия	Лабораторные работы		
1	Раздел 1. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ					ПК–6
1.1	Основы информационной безопасности	0,5			6	
1.2	Политика государства в области информационной безопасности	0,5		2	6	
1.3	Угрозы, нарушители и модель угроз безопасности информации				12	
2	Раздел 2. МЕРЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ					ПК–6
2.1	Организационные меры защиты информации	1		2	6	
2.2	Криптографические меры защиты информации	1		4	6	
2.3	Программно-технические меры защиты информации				12	
2.4	Стеганографическая и техническая защита информации				12	
3	Раздел 3. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ					ПК–6

3.1	Политика безопасности предприятия				12	
3.2	Системы обнаружения и предотвращения компьютерных атак				12	
3.3	Основные стандарты в области информационной безопасности				12	
	Итого в семестр:	**4**		**8**	**96**	
	Всего:	**4**		**8**	**96**	

в) очно-заочная форма

№ п/п	Раздел/тема	Занятия лекционного типа, (акад. часов)	Занятия семинарского типа, (акад. часов)		Самостоятельная работа, (акад. часов)	Формируемые компетенции
			Семинары и/или практические занятия	Лабораторные работы		
1	Раздел 1. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ					ПК–6
1.1	Основы информационной безопасности	2			6	
1.2	Политика государства в области информационной безопасности	2		2	6	
1.3	Угрозы, нарушители и модель угроз безопасности информации	2		2	10	
2	Раздел 2. МЕРЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ					ПК–6
2.1	Организационные меры защиты информации	2		2	6	
2.2	Криптографические меры защиты информации	2		8	4	
2.3	Программно-технические меры защиты информации	2		4	10	
2.4	Стеганографическая и техническая защита информации	2			12	
3	Раздел 3. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ					ПК–6
3.1	Политика безопасности предприятия	2			12	
3.2	Системы обнаружения и предотвращения компьютерных атак	1			12	
3.3	Основные стандарты в области информационной безопасности	1			12	
	Итого в семестр:	**18**		**18**	**90**	
	Всего:	**18**		**18**	**90**	

Программой дисциплины «Защита информации» предусмотрены занятия лекционного типа, занятия семинарского типа и самостоятельная работа обучающихся.

На занятиях семинарского типа выполняются лабораторные работы.

Самостоятельная работа предполагает изучение обучающимися теоретического курса.

Для запланированных видов занятий разработаны учебно-методические материалы, которые включены в состав электронного учебно-методического комплекса дисциплины (ЭУМКД) по дисциплине «Защита информации» [8].

5.2. Занятия лекционного типа

№ темы	Раздел/тема дисциплины	Краткое содержание лекционного занятия
1	Раздел 1. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	
1.1	Основы информационной безопасности	Понятие информации. Доступ к информации. Информационные системы. Обработка информации. Защита информации. Информационная безопасность
1.2	Политика государства в области информационной безопасности	Стратегия национальной безопасности. Доктрина информационной безопасности. Законодательство в области защиты информации.

		Государственная тайна. Коммерческая тайна. Персональные данные
1.3	Угрозы, нарушители и модель угроз безопасности информации	Понятие угрозы безопасности информации. Виды угроз безопасности информации. Источники угроз безопасности информации. Нарушители безопасности информации. Виды и цели нарушителей. Потенциал и возможности нарушителей. Способы реализации угроз нарушителем. Назначение модели угроз ИБ. Идентификация угроз безопасности информации и их источников. Модель нарушителя. Принцип оценки актуальности угроз. Оценка возможности реализации угрозы. Оценка степени ущерба. Оценка актуальности угрозы
2	Раздел 2. МЕРЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ	
2.1	Организационные меры защиты информации	Организация защиты информации. Законодательные меры защиты информации. Административные меры защиты информации. Управление рисками. Управление персоналом. Планирование действий в чрезвычайных ситуациях. Организационно-технические меры защиты информации. Физическая защита объекта информатизации. Защита поддерживающей инфраструктуры. Основные понятия контроля доступа. Идентификация, аутентификация и авторизация субъектов доступа. Модели разграничения доступа
2.2	Криптографические меры защиты информации	Понятие шифра. Шифр простой замены и его анализ. Шифры перестановки и их анализ. Варианты усложнения шифра простой замены. Шифр многоалфавитной замены и его анализ. Требования к шифрам - принцип Керхгоффса. Шифровальные машины и подходы к их анализу. Идеальный шифр и классы стойкости шифров. Требования к современным криптографическим системам. Шифры на основе сети Фейстеля. Шифры на основе SP-сети. Асимметричные системы шифрования. Схемы электронной цифровой подписи. Хэш-функции. Криптографические протоколы. Перспективы криптографии
2.3	Программно-технические меры защиты информации	Сервисы безопасности. Антивирусная защита. Типы вредоносных программ. Принципы обнаружения вредоносных программ. Выбор антивирусных средств. Межсетевое экранирование. Системы предотвращения утечки информации. Протоколирование и аудит
2.4	Стеганографическая и техническая защита информации	Исторический обзор стеганографии. Основные понятия стеганографии. Основные угрозы безопасности стеганографических систем. Типы нарушителей безопасности стеганографических систем. Типы атак на стеганографические системы. Компьютерная и цифровая стеганография. Сфера применения методов стеганографической защиты информации. Основные понятия технической защиты информации. Технические каналы утечки информации. Акустический канал утечки информации. Оптический канал утечки информации. Радиоэлектронный канал утечки информации. Принципы осуществления технической разведки. Принципы защиты от технической разведки
3	Раздел 3. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ	
3.1	Политика безопасности предприятия	Понятие политики безопасности. Назначение и содержание политики безопасности. Вопросы, рассматриваемые в политике безопасности. Организационные аспекты информационной безопасности на предприятии. Управление активами. Безопасность, связанная с управлением персоналом. Физическая безопасность. Управление доступом. Вопросы эксплуатации информационных систем. Управление инцидентами и непрерывностью бизнеса. Соответствие требованиям обязательств предприятия. Жизненный цикл политики безопасности
3.2	Системы обнаружения и предотвращения компьютерных атак	Назначение систем обнаружения и предотвращения компьютерных атак. Понятие компьютерной атаки. Требования к системам обнаружения и предотвращения компьютерных атак. Классификация систем обнаружения и предотвращения компьютерных атак. Системы анализа защищенности. Системы обнаружения атак. Системы контроля целостности. Системы анализа журналов регистрации. Размещение систем обнаружения и предотвращения атак в информационной системе. Критерии выбора систем обнаружения и предотвращения компьютерных атак.
3.3	Основные стандарты в области	Категории стандартов Российской Федерации. Основные действующие

	информационной безопасности	стандарты РФ в области информационной безопасности. Группа стандартов Р ИСО/МЭК 27000. Стандарты в области криптографической защиты информации. Стандарт Р ИСО/МЭК 15408 («Общие критерии»). Общая модель оценки безопасности информационных технологий. Функциональные компоненты безопасности. Требования доверия к безопасности. Руководящие документы уполномоченных органов (регуляторов) Российской Федерации.

5.3. Занятия семинарского типа

5.3.1. Лабораторные работы

№ темы	Раздел/тема дисциплины	Наименование и объем лабораторной работы (очная//заочная//очно-заочная формы)	Краткое содержание лабораторной работы
1	Раздел 1. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ		
1.2	Политика государства в области информационной безопасности	Стратегия национальной безопасности Российской Федерации (2/0/0 часов)	Информационное законодательство. Изучение содержания Стратегии национальной безопасности Российской Федерации
		Доктрина информационной безопасности Российской Федерации (2/0/0 часов)	Изучение содержания Доктрины информационной безопасности Российской Федерации
		Федеральный закон «О персональных данных» (2/2/2 часов)	Изучение содержания Федерального закона «О персональных данных». Анализ примера согласия на обработку персональных данных
1.3	Угрозы, нарушители и модель угроз безопасности информации	Моделирование угроз безопасности информации на примере конкретного объекта информатизации (4/0/2 часов)	Ознакомление с методическими рекомендациями по составлению модели угроз безопасности информации объекта информатизации. Самостоятельное определение актуальности угроз информационной безопасности для исследуемого объекта
2	МЕРЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ		
2.1	Организационные меры защиты информации	Парольные системы защиты (4/2/2 часов)	Изучение структуры, характеристик, сильных и слабых сторон парольных систем защиты информационных систем, закрепление на практике навыков по определению стойкости парольных систем, а также получение практических навыков реализации парольными систем
2.2	Криптографические меры защиты информации	Докомпьютерные классические шифры (4/2/4 часов)	Шифрование и дешифрование в подстановочных одноалфавитных шифрах (шифр Цезаря), подстановочных шифрах с использованием биграмм (шифр Плейфера), перестановочных шифрах. Реализация на языке программирования алгоритма шифрования и расшифрования шифром Виженера
		Анализ (взлом) шифра методом частотной атаки (2/0/0 часов)	Реализация частотной криптоатаки при анализе подстановочных шифров
		Шифрование сообщений алгоритма RSA (4/2/4 часов)	Шифрование и расшифрование алгоритмом RSA. Создание ЭЦП алгоритмом RSA. Реализация на языке программирования алгоритма RSA для шифрования и расшифрования информации

2.3	Программно-технические меры защиты информации	Работа с криптопровайдером (6/0/4 часов)	Изучения практических основ криптозащиты, основанных на программно-технических средствах защиты информации. Установка и использование КриптоПро CSP. Запрос сертификатов удостоверяющего центра и электронных подписей, генерация ключей. Подписание ЭП цифровых документов и почтовых сообщений
2.4	Стеганографическая и техническая защита информации	Стеганографическое сокрытие данных (2/0/0 часов)	Сокрытие текстовой информации в графических файлах
		Защита папок и файлов (2/0/0 часов)	Изучение методов защиты папок и файлов в операционной системе Windows
		Восстановление удаленных файлов и необратимое удаление информации (2/0/0 часов)	Восстановление удаленных файлов и необратимое удаление информации в операционной системе Windows
	Всего:	**36/8/18**	

5.4. Занятия в форме практической подготовки

Занятия в форме практической подготовки по дисциплине не организуются.

6. Оценочные материалы для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине

Оценочные материалы для текущего контроля успеваемости и промежуточной аттестации по итогам освоения дисциплины «Защита информации» сформированы в виде фонда оценочных средств (ФОС) и представлены в приложении к рабочей программе.

7. Учебно-методическое обеспечение дисциплины

7.1. Рекомендуемая литература

№ п/п	Наименование	Электронный адрес	Кол-во экз.
	7.1.1. Основная литература		
1	Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2023. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511998 (дата обращения: 07.04.2023).	https://urait.ru/bcode/511998	
2	Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512268 (дата обращения: 07.04.2023).	https://urait.ru/bcode/512268	
3	Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2023. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL:	https://urait.ru/bcode/520063	

	https://urait.ru/bcode/520063 (дата обращения: 07.04.2023).		
4	Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2023. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511138 (дата обращения: 07.04.2023).	https://urait.ru/bcode/511138	
5	Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2023. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511890 (дата обращения: 07.04.2023).	https://urait.ru/bcode/511890	
	7.1.2. Дополнительная литература		
6	Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2023. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511700 (дата обращения: 07.04.2023).	https://urait.ru/bcode/511700	
7	Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2023. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512423 (дата обращения: 07.04.2023).	https://urait.ru/bcode/512423	
8	Операционные системы [Электронный ресурс]: электронный учеб.-метод. комплекс / сост. В.В. Фирер. – Лесосибирск, 2021	http://www.lfsibgu.ru/elektronnyj-katalog	

7.2. Перечень современных профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины

№ п/п	Наименование
1.	Научно-техническая библиотека филиала СибГУ в г. Лесосибирске : [сайт]. – Лесосибирск, 2004 – . – http://lfsibgu.ru/elektronnyj-katalog. – Текст : электронный.
2.	Лань : электронно-библиотечная система издательства : [сайт]. – Москва, 2010 – . – URL: http://e.lanbook.com – Режим доступа: по подписке. – Текст : электронный.
3.	ЮРАЙТ : образовательная платформа : [сайт]. – Москва, 2013 – URL: https://urait.ru/ – Режим доступа: по подписке. – Текст : электронный.
4.	IPR SMART : цифровой образовательный ресурс: [сайт] . – Москва, 2021 – . – URL: https://www.iprbookshop.ru/ – Режим доступа: по подписке. – Текст : электронный.
5.	Сервер электронно-дистанционного обучения СибГУ им. М. Ф. Решетнева : [электрон. образоват. ресурс для студентов всех форм обучения] : [сайт]. – URL: https://dl.sibsau.ru – Режим доступа: для авториз. пользователей. – Текст : электронный.

7.3. Методические указания для обучающихся по освоению дисциплины

Программой дисциплины «Защита информации» предусмотрены занятия лекционного типа, занятия семинарского типа (лабораторные работы) и самостоятельная работа обучающихся.

Самостоятельная работа предполагает изучение теоретического курса. В период освоения дисциплины для обучающихся организуются индивидуальные и групповые консультации.

При изучении дисциплины обязательным является выполнение следующих организационных требований:

– обязательное посещение всех видов аудиторных занятий;
– ведение конспекта лекций, практических занятий;
– активная работа во время занятий;
– регулярная самостоятельная работа обучающегося в соответствии с рабочей программой дисциплины и рейтинг планом;
– своевременная сдача отчетных документов;
– получение дополнительных консультаций по подготовке, оформлению и сдаче отдельных видов заданий, в случае пропусков занятий.

Самостоятельная работа обучающегося направлена на:

– стимулирование познавательного интереса;
– систематизацию и закрепление полученных теоретических знаний;
– развитие познавательных способностей, активности, самостоятельности, ответственности и организованности обучающихся;
– формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации.

Чтобы выполнить весь объем самостоятельной работы по всем осваиваемым дисциплинам, обучающемуся необходимо заниматься по 3-5 часов ежедневно. Начинать самостоятельные внеаудиторные занятия следует с первых же дней семестра, поскольку компенсировать пропущенный материал позднее без снижения качества работы и ее производительности практически невозможно.

Вид учебных занятий	Организация деятельности обучающегося
Лекция	Лекции имеют целью дать систематизированные знания об изучаемой предметной области. В ходе лекций преподаватель излагает и разъясняет основные, наиболее сложные понятия темы, а также связанные с ней теоретические и практические проблемы, дает рекомендации на лабораторные работы и указания на самостоятельную работу. В ходе лекций обучающимся рекомендуется: – вести конспектирование учебного материала; – обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению; – задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций. Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. Для успешного овладения курсом необходимо посещать все лекции, так как тематический материал взаимосвязан между собой.
Лабораторная работа	При подготовке к лабораторным работам обучающемуся необходимо изучить методические указания по выполнению лабораторной работы, изучить основные теоретические положения по теме работы, выполнить экспериментальную часть, произвести необходимые

	расчеты, оценить правильность полученных результатов. Лабораторные работы выполняются подгруппами обучающихся в специализированных лабораториях. Каждую лабораторную работу обучающийся должен оформить в виде отчета, который представляется на рассмотрение преподавателя, защитить отчет, предоставив выполненные задания и ответив на контрольные вопросы.
Самостоятельная работа (изучение теоретической части курса)	При изучении дисциплины не все вопросы рассматриваются на лекциях и практических занятиях, часть вопросов рекомендуется преподавателем для самостоятельного изучения. При самостоятельном изучении и проработке теоретического курса необходимо повторить законспектированный во время лекции материал и дополнить его с учетом рекомендованной литературы. Важной частью самостоятельной работы является чтение учебной и научной литературы. Основная функция учебников - ориентировать обучающихся в системе знаний, умений и навыков, которые должны быть усвоены по данной дисциплине будущими специалистами. Поиск ответов на вопросы и выполнение заданий для самостоятельной работы позволяет расширить и углубить знания по курсу, применить теоретические знания в решении задач практического содержания, закрепить изученное ранее. Уровень усвоения материала может быть оценен при ответах на контрольные вопросы для самопроверки по соответствующим темам и разделам.
Подготовка к зачету	Подготовка к зачету предполагает изучение рекомендуемой литературы и других источников, конспектов лекций, повторение материалов лабораторных работ.

8. Материально-техническое обеспечение дисциплины

Наименование аудитории	Назначение аудитории	Оборудование
Учебная аудитория	для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, курсового проектирования	Учебная мебель для обучающихся, доска, рабочее место преподавателя. Комплект мультимедийного оборудования.
		Перечень лицензионного и свободно распространяемого программного обеспечения, необходимого для освоения дисциплины: 1. Операционная система Microsoft Windows Education. 2. Офисный пакет Microsoft Office. 3. Браузер Google Chrome. 4. Антивирус Dr. Web Desktop Security Suit. 5. Система программирования Microsoft Visual Studio. 6. КриптоПро.
Учебная аудитория	для проведения занятий семинарского типа (лабораторных), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, курсового проектирования	Учебная мебель для обучающихся, доска, рабочее место преподавателя.
		Компьютеры с подключением к информационно-телекоммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду СибГУ им. М.Ф. Решетнева. Перечень лицензионного и свободно распространяемого программного обеспечения, необходимого для освоения дисциплины: 1. Операционная система Microsoft Windows Education. 2. Офисный пакет Microsoft Office. 3. Браузер Google Chrome. 4. Антивирус Dr. Web Desktop Security Suit. 5. Система программирования Microsoft Visual Studio.

Помещение для самостоятельной работы	для самостоятельной работы обучающихся	Компьютеры с подключением к информационно-телекоммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду СибГУ им. М.Ф. Решетнева

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Лесосибирский филиал федерального государственного бюджетного образовательного учреждения высшего образования «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева»

ФОНД
ОЦЕНОЧНЫХ СРЕДСТВ
для проведения промежуточной аттестации
по дисциплине
(приложение к рабочей программе дисциплины)

ЗАЩИТА ИНФОРМАЦИИ

09.03.01 Информатика и вычислительная техника
Код Наименование

Направленность (профиль) образовательной программы
Программное обеспечение средств вычислительной техники и автоматизированных систем

Уровень высшего образования
бакалавриат

Форма обучения
очная, очно-заочная, заочная

Красноярск 2021

Фонд оценочных средств
для проведения промежуточной аттестации

по дисциплине Защита информации

1. Описание назначения и состава фонда оценочных средств

Настоящий фонд оценочных средств (ФОС) входит в состав рабочей программы дисциплины Защита информации

и предназначен для оценки планируемых результатов обучения по дисциплине, соотнесенных с установленными в программе индикаторами достижения компетенций.

ФОС включает в себя оценочные материалы для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся в форме: экзамена, курсовой работы.

В состав ФОС входят следующие оценочные средств:

– компьютерные тесты по темам дисциплины (текущий контроль, промежуточная аттестация);

– задания для выполнения лабораторных работ и вопросы для защиты лабораторных работ (текущий контроль).

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в программе индикаторами достижения компетенций

Код компе-тенции	Содержание компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине, соотнесенные с установленными в программе индикаторами достижения компетенции
ПК-6	Способен к проведению регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы	**ПК-6.1.** Выполняет регламентные работы по поддержке операционных систем сетевых устройств инфокоммуникационной системы **ПК-6.2.** Восстанавливает параметры программного обеспечения сетевых устройств **ПК-6.3.** Выполняет настройку сетевой инфокоммуникационной системы с точки зрения информационной безопасности	**Знать**: – общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети; – инструкции по установке и эксплуатации администрируемых сетевых устройств и программного обеспечения; – протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем **Уметь**: – использовать типовые процедуры восстановления данных; – работать с серверами архивирования и средствами управления операционных систем **Владеть**: – способами восстановления параметров при помощи средств управления специализированных операционных систем сетевого оборудования; – способами оценки эффективности конфигурации сетевых устройств с точки зрения производительности сети и защиты от несанкционированного доступа

2.1. Формы контроля формирования компетенций

№	Контролируемые раздел/тема дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1	Раздел 1. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	ПК-6	
1.1	Основы информационной безопасности		**Текущий контроль:** компьютерный тест
1.2	Политика государства в области информационной безопасности		**Текущий контроль:** компьютерный тест, задания для выполнения лабораторных работ и вопросы для защиты лабораторных работ
1.3	Угрозы, нарушители и модель угроз безопасности информации		**Текущий контроль:** компьютерный тест, задания для выполнения лабораторных работ и вопросы для защиты лабораторных работ
2	Раздел 2. МЕРЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ	ПК-6	
2.1	Организационные меры защиты информации		**Текущий контроль:** компьютерный тест, задания для выполнения лабораторных работ и вопросы для защиты лабораторных работ
2.2	Криптографические меры защиты информации		**Текущий контроль:** компьютерный тест, задания для выполнения лабораторных работ и вопросы для защиты лабораторных работ
2.3	Программно-технические меры защиты информации		**Текущий контроль:** компьютерный тест, задания для выполнения лабораторных работ и вопросы для защиты лабораторных работ
2.4	Стеганографическая и техническая защита информации		**Текущий контроль:** компьютерный тест, задания для выполнения лабораторных работ и вопросы для защиты лабораторных работ
3	Раздел 3. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ	ПК-6	
3.1	Политика безопасности предприятия		**Текущий контроль:** компьютерный тест
3.2	Системы обнаружения и предотвращения компьютерных атак		**Текущий контроль:** компьютерный тест
3.3	Основные стандарты в области информационной безопасности		**Текущий контроль:** компьютерный тест
	Промежуточная аттестация		**Промежуточный контроль:** компьютерный тест

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков владения, соотнесенных с установленными в программе индикаторами достижения компетенций

3.1. Компьютерные тесты (текущий контроль, промежуточная аттестация), формирование компетенции ПК-6

На занятиях проводятся компьютерные тесты двух видов:

– одиночные тестовые задания по ходу изложения лекционного материала (используются Google формы);
– тест по теме лекции в дистанционной среде Moodle.

Подробное описание тестовых заданий содержится в сборнике тестовых заданий, который включен в состав ЭУМКД [8].

Примеры тестовых заданий по разделу 2 «Меры обеспечения защиты информации».

1. Укажите все угрозы, для защиты от которых меры технической защиты информации рассматриваются как эффективные:

Выберите один или несколько ответов:

- Угроза нарушения доступности информации в информационной системе
- Угроза несанкционированного доступа посторонних лиц в помещения объекта информатизации
- Угроза несанкционированного съема информации, обрабатываемой техническими средствами
- Угрозы, реализуемые владельцами арендуемых хранилищ данных
- Угроза утечки речевой и видовой информации по техническим каналам

2. Укажите все криптографические методы защиты информации, используемые для обеспечения целостности информации:

Выберите один или несколько ответов:

- Системы шифрования
- Взаимная аутентификация абонентов
- Функции хэширования
- Контрольные суммы
- Схемы электронной цифровой подписи

3. Укажите всех нарушителей, для защиты от которых криптографические методы защиты информации рассматриваются как эффективные:

Выберите один или несколько ответов:

- Нарушителей, использующих средства несанкционированного получения информации, передаваемой по каналам связи
- Внутренний нарушитель, ответственный за выработку и распространение криптографических ключей
- Нарушитель, использующий средства несанкционированного получения информации, обрабатываемой техническими средствами в открытом виде
- Нарушитель, обладающий значительными вычислительными ресурсами

4. Укажите все мероприятия, которые включают организационно-технические меры ЗИ:

Выберите один или несколько ответов:

- Защита объекта информатизации от стихийных угроз
- Введение пропускного режима на территории предприятия
- Экранирование помещений обработки конфиденциальных сведений
- Разработка регламентов действий персонала в чрезвычайных ситуациях

5. Укажите все документы, относящиеся к координирующим мерам ЗИ:

Выберите один или несколько ответов:

- Руководящие документы ФСТЭК
- Кодекс об административных правонарушениях
- Закон о коммерческой тайне
- Уголовный кодекс

6. Программно-технические меры защиты информации рассматриваются как потенциально уязвимые для внешнего нарушителя, обладающего:

Выберите один ответ:

- Средствами несанкционированного съема информации

- Достаточным запасом времени
- Высокой квалификацией
- Значительными вычислительными мощностями

7. По способам осуществления меры обеспечения защиты информации подразделяются на:

Выберите один ответ:

- Законодательные, морально-этические, административные, организационные, программно-технические
- Законодательные, морально-этические, административные, организационно-технические
- Организационные, криптографические, меры технической ЗИ, стеганографические
- Законодательные, морально-этические, административные, организационно-технические, программно-технические

8. К стеганографическим методам защиты информации, предназначенным для обеспечения целостности информации, относится:

Выберите один ответ:

- Сокрытие данных в неиспользуемых (зарезервированных) областях форматов файлов
- Сокрытие информации в аудио файлах
- Использование цифровых водяных знаков
- Электронная цифровая подпись

9. Перечислите следующие элементы в порядке их следования в принципиальной схеме работы системы шифрования (без повторов, в порядке первого упоминания при следовании от начала к концу схемы). В ответе запишите последовательность цифр без запятых и пробелов (например: 1234): 1. Шифртекст. 2. Алгоритм зашифрования. 3.Открытый текст (сообщение). 4. Алгоритм расшифрования.

10. Укажите все источники законодательных мер защиты информации,распространяющихся на всех участников информационных отношений, в Российской Федерации:

- Выберите один или несколько ответов:
- Приказы уполномоченных федеральных служб
- Указы федеральных органов исполнительной власти
- Международные договоры РФ
- Распоряжения и приказы министерств РФ

11. Категории криптографических и стеганографических мер защиты информации в классификации по принципу действия соответствуют в классификации по способам осуществления категории:

Выберите один ответ:

- Алгоритмических мер ЗИ
- Организационно-технических мер ЗИ
- Программно-технических мер ЗИ
- Технических мер ЗИ

12. В задачи организационных мер защиты информации входит:

Выберите один ответ:

- Защита от компьютерных атак, осуществляемых по информационно-телекоммуникационным сетям
- Создание условий обеспечения и контроля соблюдения регламентов и правил

- Регламентирование действий посетителей на территории объекта информатизации
- Противодействие несанкционированному съему информации, обрабатываемой техническими средствами

13. Совокупность людей, процедур и оборудования, защищающих объект информатизации от действий, нарушающих его безопасность представляет собой

Выберите один ответ:

- Программно-технический комплекс защиты информации
- Систему физической защиты
- Организационно-технические меры защиты информации
- Систему комплексной защиты информации

14. Разработка политики безопасности предусматривается в рамках

Выберите один ответ:

- Программно-технических мер ЗИ
- Морально-этических мер ЗИ
- Организационно-технических мер ЗИ
- Административных мер ЗИ

15. Укажите все задачи, для решения которых программно-технические средства защиты информации рассматриваются как эффективные:

Выберите один или несколько ответов:

- Противодействие несанкционированному съему информации по техническим каналам
- Минимизации вероятности угроз, реализованных по причине халатности или недостаточной квалификации
- Защита от нарушителей, обладающих значительными вычислительными ресурсами
- Защита информации, передаваемой за пределы контролируемой территории объекта информатизации

16. Права и обязанности участников информационных отношений устанавливают

Выберите один ответ:

- Административно-правовые меры ЗИ
- Организационные меры ЗИ
- Законодательные меры ЗИ
- Административные меры ЗИ

17. Любые действующие на территории объекта информатизации правила, регламентирующие доступ к информации и порядок работы с ней, вместе с мерами обеспечения и контроля исполнения таких правил, составляют:

Выберите один ответ:

- Координирующие меры ЗИ
- Организационные меры ЗИ
- Административные меры ЗИ
- Организационно-технические меры ЗИ

18. Укажите все мероприятия, которые включают административные меры защиты информации:

Выберите один или несколько ответов:

- Защита объекта информатизации от техногенных и стихийных угроз
- Обучение и инструктаж персонала
- Установление пропускного режима на территории предприятия
- Выбор методов и средств защиты информации в организации

- Оценка угроз безопасности информации

19. Стеганографические меры защиты информации являются наиболее эффективными по сравнению с другими мерами защиты информации для

Выберите один ответ:

- Сохранения целостности передаваемой информации
- Контроля соблюдения условий лицензий
- Исключения действий внутренних нарушителей
- Обеспечения конфиденциальности связи между особо важными абонентами

20. Укажите все основные принципы разграничения доступа сотрудников к ресурсам ИС:

Выберите один или несколько ответов:

- Ограничение доступа
- Минимизация полномочий
- Разделение обязанностей
- Централизация управления

Для проведения промежуточной аттестации используется тест, составленный из вопросов тестов текущего контроля, по одному вопросу из каждой темы (случайный выбор). Для проведения тестирования используется дистанционная среда Moodle.

Примеры тестовых заданий для промежуточной аттестации.

1. Что такое аутентификация?
2. Как реализован S-слой (замена) в шифре «Кузнечик», основанном на SP-сети.
3. Назовите государственный стандарт на процессы формирования и проверки электронной цифровой подписи.
4. Назовите максимально допустимый уровень проектной защищенности, согласно Методике определения угроз безопасности информации в информационных системах, разработанной ФСТЭК в 2015 г.
5. В чем заключается запуск системы с ограниченными полномочиями.
6. Что такое компьютерная стеганография?
7. Как называется комплекс взаимосвязанных обслуживающих структур или объектов, составляющих и (или) обеспечивающих основу функционирования информационной системы?
8. Определите место информационной безопасности в национальной безопасности Российской Федерации как одной из ее составных частей.
9. Как называется метод обнаружения вредоносных программ, суть которого заключается в поиске участков кода исполняемого объекта, отвечающих за конкретные вредоносные действия?
10. На сложности какой задачи основывается надежность криптографической системы RSA?
11. Перечислите все возможные цели (мотивы), согласно Методике определения угроз безопасности информации в информационных системах, разработанной ФСТЭК в 2015 г., предусмотренные для нарушителя вида «Пользователи информационной системы».
12. Что понимают под зондированием как способом выявления уязвимостей эксплуатации?
13. Частью какого шифра является поиск пар одинаковых подстрок в шифртексте и вычисление расстояния между их одинаковыми элементами.
14. В чем заключается преимущество оптического канала утечки информации по сравнению с другими каналами, с точки зрения нарушителя?
15. На чем основан стеганографический метод наименьших значащих бит?

16. Укажите все категории мер, принятие которых, согласно закону «Об информации, информационных технологиях и о защите информации», представляет собой защита информации.

17. Перечислите все мероприятия, которые включают административные меры защиты информации.

18. Укажите все основания для проведения переоценки угроз безопасности информации, согласно Методике определения угроз безопасности информации в информационных системах, разработанной ФСТЭК в 2015 г.

19. Перечислите все процессы, при которых, согласно рекомендации по обеспечению соответствия требованиям обязательств организации, должны учитываться требования безопасности.

20. Перечислите все ситуации, в которых указывается на нарушение целостности информации.

21. Перечислите все угрозы, застрагивающие доступность информации

22. Укажите все уязвимости, присущие любой системе контроля и разграничения доступа на основе принципов ее работы.

3.2. Задания для лабораторных работ на занятиях семинарского типа и вопросы для защиты лабораторных работ (текущий контроль), формирование компетенции ПК-6

Подробное описание лабораторных работ и вопросов для защиты лабораторных работ содержатся в Практикуме по выполнению лабораторных работ, который включен в состав ЭУМКД [8].

Примерные задания для лабораторной работы «Парольные системы защиты» по теме «Организационные методы защиты информации».

Задание 1. Определить время перебора всех словарных паролей (объем словаря равен 1000000 слов), если скорость перебора составляет 100 паролей/секунду.

Задание 2 Определить время перебора всех паролей с параметрами. Алфавит состоит из A символов. Длина пароля символов L. Скорость перебора V паролей в секунду. После каждого из m неправильно введенных паролей идет пауза в v секунд.

Задание 3. Определить минимальную длину пароля, алфавит которого состоит из A символов, время перебора которого было не меньше T лет. Скорость перебора V паролей в секунду.

Задание 4. Определить количество символов алфавита, пароль состоит из L символов, время перебора которого было не меньше T лет. Скорость перебора V паролей в секунду.

Задание 5. Написать программу, которая должна эмулировать работу парольной системы защиты. Программа должна реализовывать 5 из 10 требований, предъявляемых к парольным системам защиты.

Перечень вопросов для защиты лабораторной работы «Парольные системы защиты» по теме «Организационные методы защиты информации».

1. Что такое парольная система защиты информации?
2. Какие реализации парольных систем защиты информации существуют?
3. Перечислите требования к выбору и использованию паролей.
4. В каких режимах злоумышленник может реализовать угрозы парольной системы?

4. Описание показателей, критериев, шкал оценивания планируемых результатов обучения по дисциплине, соотнесенных с установленными в программе индикаторами достижения компетенций

4.1. Показатели и критерии оценивания заданий для лабораторных работ и вопросов для защиты лабораторных работ

Оценка	Показатели оценивания	Критерии оценивания
«5» (отлично)	Качество выполнения всех заданий лабораторных работ; полнота и правильность ответов на контрольные вопросы; оформление в соответствии с требованиями, самостоятельность выполнения, сдача лабораторных работ в установленные сроки.	Выполнены без замечаний все задания лабораторных работ; даны полные правильные ответы на контрольные вопросы; лабораторные работы выполнены самостоятельно, сданы в срок, оформлены в соответствии с требованиями
«4» (хорошо)		Задания лабораторных работ выполнены с несущественными замечаниями; недостаточно полные ответы на контрольные вопросы; лабораторные работы выполнены самостоятельно, сданы в срок, оформлены в соответствии с требованиями
«3» (удовлетворительно)		Задания лабораторных работ выполнены с существенными замечаниями, устраненными во время контактной работы с преподавателем; ошибки в ответах на контрольные вопросы; лабораторные работы выполнены с нарушениями графика, в оформлении работ есть недостатки; работы выполнены самостоятельно
«2» (неудовлетворительно)		Часть лабораторных работ или все работы выполнены из фрагментов работ других авторов и носят несамостоятельный характер; задания выполнены не полностью или неправильно; оформление работ не соответствует требованиям

4.2. Показатели и критерии оценивания задания в тестовой форме

Код	Вид оценочного средства	Критерии	Балл	Максимальный балл 5 – минимальный балл 1
Т.1	Тестовое задание №	выставляется студенту если 86-100% тестовых вопросов/заданий выполнено правильно	5	**5 – 3**
		выставляется студенту если 70-85% тестовых задач/заданий выполнено правильно	4	
		выставляется студенту если 50-69% тестовых задач/заданий выполнено правильно	3	
		при ответе студента менее чем на 60% вопросов, тестовое задание не зачитывается и у студента образуется долг, который должен быть закрыт в течении семестра или на зачетной неделе	н/з	

Минимальный балл, который необходимо набрать для зачета, равен 3.

5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Для проверки качества освоения программы дисциплины и оценки результатов обучения по дисциплине, соотнесенных с установленными в программе индикаторами достижения компетенции проводится текущий контроль успеваемости и промежуточная аттестация обучающихся в форме зачета.

Контроль успеваемости обучающихся осуществляется с использованием рейтинговой системы оценки успеваемости обучающихся.

Текущий контроль проводится регулярно на всех видах групповых занятий по дисциплине. В конце семестра на основании поэтапного контроля процесса обучения суммируются баллы текущих, рубежных рейтингов (контрольные недели), подсчитываются дополнительные баллы (за посещаемость и активность на занятиях).

Результаты рейтинговой аттестации объявляются преподавателем на последнем занятии в зачетную неделю и служат основой для итогового результата промежуточной аттестации обучающегося по дисциплине.

5.1. Соответствие балльной шкалы оценок по дисциплине уровню сформированности компетенций обучающегося

Уровень сформированности компетенций	Оценка	Пояснение
Высокий	«5» (отлично) зачтено	Теоретическое содержание курса освоено полностью, без пробелов, все предусмотренные программой обучения учебные задания выполнены, планируемые результаты обучения по дисциплине, соотнесенные с установленными в программе индикаторами достижения компетенций, достигнуты.
Выше среднего	«4» (хорошо) зачтено	Теоретическое содержание курса освоено полностью, все предусмотренные программой обучения учебные задания выполнены с незначительными замечаниями, планируемые результаты обучения по дисциплине, соотнесенные с установленными в программе индикаторами достижения компетенций, достигнуты.
Средний	«3» (удовлетворительно) зачтено	Теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, большинство предусмотренных программой обучения учебных задач выполнено, но отмечены ошибки, планируемые результаты обучения по дисциплине, соотнесенные с установленными в программе индикаторами достижения компетенций, в целом достигнуты.
Неудовлетворительный	«2» (не удовлетворительно) не зачтено	Теоретическое содержание курса не освоено, большинство предусмотренных программой обучения учебных заданий либо не выполнено, либо содержит грубые ошибки; дополнительная самостоятельная работа над материалом не приведет к какому-либо значимому повышению качества выполнения учебных заданий. Планируемые результаты обучения по дисциплине, соотнесенные с установленными в программе индикаторами достижения компетенций, не достигнуты.

ЛИСТ РЕГИСТРАЦИИ ОБНОВЛЕНИЙ (АКТУАЛИЗАЦИИ)

Рабочей программы дисциплины «Защита информации» по направлению подготовки 09.03.01 «Информатика и вычислительная техника» направленность образовательной программы «Программное обеспечение средств вычислительной техники и автоматизированных систем»

№ п/п	Раздел (подраздел), в который вносятся изменения	Основание для изменения	Краткая характеристика вносимых изменений
1	Пункт 7.1. Рекомендуемая литература		
2	Пункт 7.2. Перечень современных профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины		
3	Пункт 8. Перечень оборудования и технических средств обучения, необходимых для осуществления образовательного процесса по дисциплине		

Протокол заседания кафедры _____

от «___» _____ 202 г. № ___

Зав. кафедрой _____