МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины (модуля)

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специальность и специализация
10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2026

Форма обучения
очная

Владивосток 2026

Рабочая программа дисциплины (модуля) «Основы информационной безопасности» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем (утв. приказом Минобрнауки России от 26.11.2020г. №1457) и Порядком организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры (утв. приказом Минобрнауки России от 06.04.2021 г. N245).

Составитель(и):

Мартышенко Н.С.

Шумик Е.Г.

Утверждена на заседании кафедры информационной безопасности от 14.05.2026 , протокол № 8

СОГЛАСОВАНО:

Заведующий кафедрой (разработчика)

Шумик Е.Г.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат	eg_1575874368
Номер транзакции	0000000000FAF467
Владелец	Шумик Е.Г.

1 Цель, планируемые результаты обучения по дисциплине (модулю)

Целью освоения дисциплины «Основы информационной безопасности» является формирование у студентов системы знаний в области информационной безопасности и применения на практике методов и средств защиты информации.

Задачи освоения дисциплины: формирование умения обеспечить защиту информации и объектов информатизации; формирование умения составлять заявительную документацию в надзорные государственные органы инфокоммуникационной отрасли; формирование навыков выполнения работ в области технического регулирования, сертификации технических средств, систем, процессов, оборудования и материалов; формирование навыков обеспечения защиты объектов интеллектуальной собственности и результатов исследований и разработок как коммерческой тайны предприятия; настройка и обслуживание аппаратно-программных средств.

Планируемыми результатами обучения по дисциплине (модулю), являются знания, умения, навыки. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы, представлен в таблице 1.

Таблица 1 – Компетенции, формируемые в результате изучения дисциплины (модуля)

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине		
			Код результата	Формулировка результата	
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)	ОПК-1 : Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1.1к : Понимает принципы теории информационной безопасности и проблемы государственной и региональной информационной безопасности	РД1	Знание	современных законов, стандартов, методов и технологий в области защиты информации
			РД2	Знание	требований к защите информации определенного типа
			РД3	Умение	использовать современные программно-аппаратные средства защиты информации
		ОПК-1.2к : Оценивает роль информации, информационной безопасности в современном обществе, их значение обеспечения объективных потребностей личности, общества и государства	РД4	Умение	обеспечивать защиту информации
			РД5	Навык	владения современными методами обеспечения защиты информации
	ОПК-5.1 : Способен разрабатывать и реализовывать	ОПК-5.1.1к : Определяет источники информации,	РД10	Умение	управлять информационной безопасностью организации

	политику информационной безопасности открытых информационных систем;	регламентирующие деятельность, связанную с организацией политики безопасности	РД11	Навык	владения методами оценки рисков информационной безопасности
			РД6	Знание	современных методов и средств защиты информации
			РД7	Умение	анализировать информационную безопасность организации
			РД8	Навык	владения современными технологиями и методами обеспечения информационной безопасности организации
			РД9	Знание	современных технологий, методик и средств защиты информации

В процессе освоения дисциплины решаются задачи воспитания гармонично развитой, патриотичной и социально ответственной личности на основе традиционных российских духовно-нравственных и культурно-исторических ценностей, представленные в таблице 1.2.

Таблица 1.2 – Целевые ориентиры воспитания

Воспитательные задачи	**Формирование ценностей**	**Целевые ориентиры**
Формирование гражданской позиции и патриотизма		
Воспитание уважения к Конституции и законам Российской Федерации	Гражданственность	Дисциплинированность
Формирование духовно-нравственных ценностей		
Воспитание чувства долга и ответственности перед семьей и обществом	Высокие нравственные идеалы	Осознание ценности профессии
Формирование научного мировоззрения и культуры мышления		
Развитие познавательного интереса и стремления к знаниям	Служение Отечеству и ответственность за его судьбу	Соблюдение моральных принципов
Формирование коммуникативных навыков и культуры общения		
Развитие умения эффективно общаться и сотрудничать	Взаимопомощь и взаимоуважение	Способность находить, анализировать и структурировать информацию

2 Место дисциплины (модуля) в структуре ОПОП

Дисциплина «Основы информационной безопасности» относится к базовой части «Блока 1Дисциплины (модули)» учебного плана специальности 10.05.03 «Информационнаябезопасность автоматизированных систем».Входными требованиями, необходимыми для освоения дисциплины, является наличие у обучающихся компетенций, сформированных при изучении дисциплин и/илипрохождении практик «Алгебра и геометрия», «Информатика», «Основы информационной безопасности». На данную дисциплинуопираются «Криптографические методы защиты информации», «Угрозы информационной безопасности автоматизированных систем» и др.

3. Объем дисциплины (модуля)

Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу с обучающимися (по видам учебных занятий) и на самостоятельную работу, приведен в таблице 2.

Таблица 2 – Общая трудоемкость дисциплины

Название ОПОП ВО	Форма обуче-ния	Часть УП	Семестр (ОФО) или курс (ЗФО, ОЗФО)	Трудо-емкость	Объем контактной работы (час)						СРС	Форма аттес-тации
				(З.Е.)	Всего	Аудиторная			Внеауди-торная			
						лек.	прак.	лаб.	ПА	КСР		
10.05.03 Информационная безопасность автоматизированных систем	ОФО	С1.Б	3	4	73	18	36	0	1	18	71	Э

4 Структура и содержание дисциплины (модуля)

4.1 Структура дисциплины (модуля) для ОФО

Тематический план, отражающий содержание дисциплины (перечень разделов и тем), структурированное по видам учебных занятий с указанием их объемов в соответствии с учебным планом, приведен в таблице 3.1

Таблица 3.1 – Разделы дисциплины (модуля), виды учебной деятельности и формы текущего контроля для ОФО

№	Название темы	Код ре-зультата обучения	Кол-во часов, отведенное на				Форма текущего контроля
			Лек	Практ	Лаб	СРС	
1	Введение в информационную безопасность	РД1, РД2, РД4, РД6, РД7, РД9	4	6	0	15	Тест, выполнение практического задания
2	Правовое обеспечение информационной безопасности	РД1, РД2, РД6, РД7	2	6	0	15	Тест, выполнение практического задания
3	Организационное обеспечение информационной безопасности	РД1, РД6, РД10, РД11	2	6	0	15	Тест, выполнение практического задания

4	Технические средства и методы защиты информации	РД5, РД6, РД8, РД9, РД10, РД11	4	6	0	15	Тест, выполнение практического задания
5	Программно-аппаратные средства и методы обеспечения информационной безопасности	РД3, РД5, РД6, РД8, РД9, РД10, РД11	4	6	0	15	Тест, выполнение практического задания
6	Криптографические методы защиты информации	РД5, РД6, РД9, РД10, РД11	2	6	0	15	Тест, выполнение практического задания
Итого по таблице			**18**	**36**	**0**	**90**	

4.2 Содержание разделов и тем дисциплины (модуля) для ОФО

Тема 1 Введение в информационную безопасность.

Содержание темы: Информационная безопасность. Основные понятия. Модели информационной безопасности. Виды защищаемой информации.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекционное занятие, практическое занятие.

Виды самостоятельной подготовки студентов по теме: Подготовка к контрольным вопросам собеседования, подготовка к промежуточной аттестации.

Тема 2 Правовое обеспечение информационной безопасности.

Содержание темы: Основные нормативно-правовые акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекционное занятие, практическое занятие.

Виды самостоятельной подготовки студентов по теме: Подготовка к контрольным вопросам собеседования, подготовка к промежуточной аттестации.

Тема 3 Организационное обеспечение информационной безопасности.

Содержание темы: Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. Экономическая безопасность предприятия.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекционное занятие, практическое занятие.

Виды самостоятельной подготовки студентов по теме: Подготовка к контрольным вопросам собеседования, подготовка к промежуточной аттестации.

Тема 4 Технические средства и методы защиты информации.

Содержание темы: Инженерная защита объектов. Защита информации от утечки по техническим каналам.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекционное занятие, практическое занятие.

Виды самостоятельной подготовки студентов по теме: Подготовка к контрольным вопросам собеседования, подготовка к промежуточной аттестации.

Тема 5 Программно-аппаратные средства и методы обеспечения информационной безопасности.

Содержание темы: Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекционное занятие, практическое занятие.

Виды самостоятельной подготовки студентов по теме: Подготовка к контрольным вопросам собеседования, подготовка к промежуточной аттестации.

Тема 6 Криптографические методы защиты информации.

Содержание темы: Симметричные и ассиметричные системы шифрования. Цифровые подписи (Электронные подписи). Инфраструктура открытых ключей. Криптографические протоколы.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекционное занятие, практическое занятие.

Виды самостоятельной подготовки студентов по теме: Подготовка к контрольным вопросам собеседования, подготовка к промежуточной аттестации.

5 Методические указания для обучающихся по изучению и реализации дисциплины (модуля)

5.1 Методические рекомендации обучающимся по изучению дисциплины и по обеспечению самостоятельной работы

Самостоятельная работа студентов (СРС) — это деятельность учащихся, которуюони совершают без непосредственной помощи и указаний преподавателя, руководствуясьсформировавшимися ранее представлениями о порядке и правильности выполненияопераций. Цель СРС в процессе обучения заключается, как в усвоении знаний, так и вформировании умений и навыков по их использованию в новых условиях на новом учебномматериале. Самостоятельная работа призвана обеспечивать возможность осуществлениястудентами самостоятельной познавательной деятельности в обучении, и является видомучебного труда, способствующего формированию у студентов самостоятельности. Вданной учебной программе приведен перечень основных и дополнительных источников,которые предлагается изучить в процессе облучения по дисциплине. Кроме того, длярасширения и углубления знаний по данной дисциплине целесообразно использовать:научные публикации в тематических журналах; полнотекстовые базы данных библиотеки;имеющиеся в библиотеках вуза и региона публикаций на электронных и бумажныхносителях. Успешное освоение дисциплины предполагает активную работу студентов навсех занятиях аудиторной формы: лекций и практических занятий, выполнениеаттестационный мероприятий, эффективную самостоятельную работу.

5.2 Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов

При необходимости обучающимся из числа лиц с ограниченными возможностями здоровья и инвалидов (по заявлению обучающегося) предоставляется учебная информация в доступных формах с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания, консультации и др.

- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания, консультации и др.

- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; индивидуальные задания, консультации и др.

6 Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

В соответствии с требованиями ФГОС ВО для аттестации обучающихся на соответствие их персональных достижений планируемым результатам обучения по дисциплине (модулю) созданы фонды оценочных средств. Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 1.

7 Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература

1. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2023. — 400 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1912992 (дата обращения: 31.05.2026)

2. Мельников, А. В. Основы информационной безопасности : учебное пособие / А. В. Мельников, С. В. Зарубин. – Москва : РГУП, 2025. - 220 с. – ISBN 978-5-00209-188-1. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2228306 (дата обращения: 31.05.2026)

3. Раченко, Т. А. Информационная безопасность : учебно-методическое пособие / Т. А. Раченко. — Тольятти : ТГУ, 2024. — 135 с. — ISBN 978-5-8259-1612-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/427130 (дата обращения: 25.05.2026). — Режим доступа: для авториз. пользователей.

7.2 Дополнительная литература

1. Программно-аппаратная защита информации : Учебное пособие [Электронный ресурс] : Издательство ФОРУМ , 2019 - 352 - Режим доступа: https://znanium.com/catalog/document?id=340852

2. Раченко, Т. А. Информационная безопасность : учебно-методическое пособие / Т. А. Раченко. — Тольятти : ТГУ, 2024. — 135 с. — ISBN 978-5-8259-1612-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/427130 (дата обращения: 25.05.2026). — Режим доступа: для авториз. пользователей.

7.3 Ресурсы информационно-телекоммуникационной сети "Интернет", включая профессиональные базы данных и информационно-справочные системы (при необходимости):

1. СПС КонсультантПлюс - Режим доступа: http://www.consultant.ru/
2. Электронная библиотечная система ZNANIUM.COM - Режим доступа: https://znanium.com/
3. Электронно-библиотечная система "ZNANIUM.COM"
4. Электронно-библиотечная система "ЛАНЬ"
5. Open Academic Journals Index (OAJI). Профессиональная база данных - Режим доступа: http://oaji.net/
6. Президентская библиотека им. Б.Н.Ельцина (база данных различных профессиональных областей) - Режим доступа: https://www.prlib.ru/

8 Материально-техническое обеспечение дисциплины (модуля) и перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

Основное оборудование:

- Мульт. медийный комплект № 2: Проектор Panasonic PT-LX26HE, потолочное крепление Tuarex Corsa, клеммный модуль Kramer WX -1N, коннектор VGA, экран Lumien Ecopicture
- Персональный компьютер №1 "B-tronix professional 3872\2015"

Программное обеспечение:

- Microsoft Windows 7 Ultimate Russian
- VMware Workstation 9 for Linux andWindows

МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Фонд оценочных средств
для проведения текущего контроля
и промежуточной аттестации по дисциплине (модулю)

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специальность и специализация
10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2026

Форма обучения
очная

Владивосток 2026

1 Перечень формируемых компетенций

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)	ОПК-1 : Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1.1к : Понимает принципы теории информационной безопасности и проблемы государственной и региональной информационной безопасности
		ОПК-1.2к : Оценивает роль информации, информационной безопасности в современном обществе, их значение обеспечения объективных потребностей личности, общества и государства
	ОПК-5.1 : Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем;	ОПК-5.1.1к : Определяет источники информации, регламентирующие деятельность, связанную с организацией политики безопасности

Компетенция считается сформированной на данном этапе в случае, если полученные результаты обучения по дисциплине оценены положительно (диапазон критериев оценивания результатов обучения «зачтено», «удовлетворительно», «хорошо», «отлично»). В случае отсутствия положительной оценки компетенция на данном этапе считается несформированной.

2 Показатели оценивания планируемых результатов обучения

Компетенция ОПК-1 «Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства»

Таблица 2.1 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ОПК-1.1к : Понимает принципы теории информационной безопасности и проблемы государственной и региональной информационной безопасности	РД 1	Знание	современных законов, стандартов, методов и технологий в области защиты информации	Сформировавшееся систематическое знание современных законов, стандартов, методов и технологий в области защиты информации
	РД 2	Знание	требований к защите информации определенного типа	Сформировавшееся систематическое знание требований к защите информации определенного типа
	РД 3	Умение	использовать современные программно-аппаратные средства защиты информации	Сформировавшееся систематическое умение использовать современные программно-аппаратные средства защиты информации
ОПК-1.2к : Оценивает роль информации, информационной безопасности в современном обществе, их значение обеспе	РД 4	Умение	обеспечивать защиту информации	Сформировавшееся систематическое умение обеспечивать защиту информации

чения объективных потребностей личности, общества и государства	РД 5	Навык	владения современными методами обеспечения защиты информации	Сформировавшееся систематическое владение современными методами обеспечения защиты информации

Компетенция ОПК-5.1 «Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем;»

Таблица 2.2 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ОПК-5.1.1к : определяет источники информации, регламентирующие деятельность, связанную с организацией политики безопасности	РД 6	Знание	современных методов и средств защиты информации	Сформировавшееся систематическое знание современных методов и средств защиты информации
	РД 7	Умение	анализировать информационную безопасность организации	Сформировавшееся систематическое умение анализировать информационную безопасность организации
	РД 8	Навык	владения современными технологиями и методами обеспечения информационной безопасности организации	Сформировавшееся систематическое владение современными технологиями и методами обеспечения информационной безопасности организации
	РД 9	Знание	современных технологий, методик и средств защиты информации	Сформировавшееся систематическое знание современных технологий, методик и средства защиты информации
	РД 10	Умение	управлять информационной безопасностью организации	Сформировавшееся систематическое умение управлять информационной безопасностью организации
	РД 11	Навык	владения методами оценки рисков информационной безопасности	Сформировавшееся систематическое владение методами оценки рисков информационной безопасности

Таблица заполняется в соответствии с разделом 1 Рабочей программы дисциплины (модуля).

3 Перечень оценочных средств

Таблица 3 – Перечень оценочных средств по дисциплине (модулю)

Контролируемые планируемые результаты обучения	Контролируемые темы дисциплины	Наименование оценочного средства и представление его в ФОС	
		Текущий контроль	Промежуточная аттестация
Очная форма обучения			

РД1	Знание : современных законов, стандартов, методов и технологий в области защиты информации	1.1. Введение в информационную безопасность	Тест	Экзамен в устной форме
		1.2. Правовое обеспечение информационной безопасности	Тест	Экзамен в устной форме
		1.3. Организационное обеспечение информационной безопасности	Тест	Экзамен в устной форме
РД2	Знание : требований к защите информации определенного типа	1.1. Введение в информационную безопасность	Тест	Экзамен в устной форме
		1.2. Правовое обеспечение информационной безопасности	Тест	Экзамен в устной форме
РД3	Умение : использовать современные программно-аппаратные средства защиты информации	1.5. Программно-аппаратные средства и методы обеспечения информационной безопасности	Практическая работа	Экзамен в устной форме
РД4	Умение : обеспечивать защиту информации	1.1. Введение в информационную безопасность	Практическая работа	Экзамен в устной форме
РД5	Навык : владения современными методами обеспечения защиты информации	1.4. Технические средства и методы защиты информации	Практическая работа	Экзамен в устной форме
		1.5. Программно-аппаратные средства и методы обеспечения информационной безопасности	Практическая работа	Экзамен в устной форме
		1.6. Криптографические методы защиты информации	Практическая работа	Экзамен в устной форме
РД6	Знание : современных методов и средств защиты информации	1.1. Введение в информационную безопасность	Практическая работа	Экзамен в устной форме
		1.2. Правовое обеспечение информационной безопасности	Практическая работа	Экзамен в устной форме
		1.3. Организационное обеспечение информационной безопасности	Практическая работа	Экзамен в устной форме
		1.4. Технические средства и методы защиты информации	Практическая работа	Экзамен в устной форме
		1.5. Программно-аппаратные средства и методы обеспечения информационной безопасности	Практическая работа	Экзамен в устной форме
		1.6. Криптографические методы защиты информации	Практическая работа	Экзамен в устной форме
РД7	Умение : анализировать информационную безопасность организации	1.1. Введение в информационную безопасность	Практическая работа	Экзамен в устной форме
		1.2. Правовое обеспечение информационной безопасности	Практическая работа	Экзамен в устной форме
РД8	Навык : владения современными технологиями и методами обеспечения информационной безопасности организации	1.4. Технические средства и методы защиты информации	Практическая работа	Экзамен в устной форме
		1.5. Программно-аппаратные средства и методы	Практическая работа	Экзамен в устной форме

		обеспечения информационной безопасности		
РД9	Знание : современных технологий, методик и средств защиты информации	1.1. Введение в информационную безопасность	Тест	Экзамен в устной форме
		1.4. Технические средства и методы защиты информации	Тест	Экзамен в устной форме
		1.5. Программно-аппаратные средства и методы обеспечения информационной безопасности	Тест	Экзамен в устной форме
		1.6. Криптографические методы защиты информации	Тест	Экзамен в устной форме
РД10	Умение : управлять информационной безопасностью организации	1.3. Организационное обеспечение информационной безопасности	Практическая работа	Экзамен в устной форме
		1.4. Технические средства и методы защиты информации	Практическая работа	Экзамен в устной форме
		1.5. Программно-аппаратные средства и методы обеспечения информационной безопасности	Практическая работа	Экзамен в устной форме
		1.6. Криптографические методы защиты информации	Практическая работа	Экзамен в устной форме
РД11	Навык : владения методами оценки рисков информационной безопасности	1.3. Организационное обеспечение информационной безопасности	Практическая работа	Экзамен в устной форме
		1.4. Технические средства и методы защиты информации	Практическая работа	Экзамен в устной форме
		1.5. Программно-аппаратные средства и методы обеспечения информационной безопасности	Практическая работа	Экзамен в устной форме
		1.6. Криптографические методы защиты информации	Практическая работа	Экзамен в устной форме

4 Описание процедуры оценивания

Качество сформированности компетенций на данном этапе оценивается по результатам текущих и промежуточных аттестаций при помощи количественной оценки, выраженной в баллах. Максимальная сумма баллов по дисциплине (модулю) равна 100 баллам.

Вид учебной деятельности	Оценочное средство			
	Тест	Практические задания	Экзамен	Итого
Лекционные занятия	20			20
Практические занятия		40		60
Промежуточная аттестация			20	20
Итого	40	40	20	100

Сумма баллов, набранных студентом по всем видам учебной деятельности в рамках дисциплины, переводится в оценку в соответствии с таблицей.

Сумма баллов по дисциплине	Оценка по промежуточной аттестации	Характеристика качества сформированности компетенции
от 91 до 100	«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций, обнаруживает всестороннее, систематическое и глубокое знание учебного материала, усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой, умеет свободно выполнять практические задания, предусмотренные программой, свободно оперирует приобретенными знаниями, умениями, применяет их в ситуациях повышенной сложности.
от 76 до 90	«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
от 61 до 75	«зачтено» / «удовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций: в ходе контрольных мероприятий допускаются значительные ошибки, проявляется отсутствие отдельных знаний, умений, навыков по некоторым дисциплинарным компетенциям, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.
от 41 до 60	«не зачтено» / «неудовлетворительно»	У студента не сформированы дисциплинарные компетенции, проявляется недостаточность знаний, умений, навыков.
от 0 до 40	«не зачтено» / «неудовлетворительно»	Дисциплинарные компетенции не сформированы. Проявляется полное или практически полное отсутствие знаний, умений, навыков.

5 Примерные оценочные средства

5.1 Примерный перечень вопросов по темам

1. Что такое информационная безопасность?
2. Перечислите основные угрозы информационной безопасности.
3. Какие существуют модели информационной безопасности?
4. Какие методы защиты информации выделяют?
5. Право. Источники права.
6. Какие основные законы в области защиты информации в РФ?
7. Охарактеризуйте биометрические данные как персональные данные.
8. Что такое профессиональная тайна?Что такое служебная тайна?
9. Что такое коммерческая тайна?
10. Какие основные международные стандарты в области информационной безопасности?
11. «Оранжевая книга»ISO/IEC 15408.
12. Как связаны международные стандарты и стандарты РФ?
13. СТО БР ИББС-1.1-2007. «Аудит информационной безопасности».
14. РС БР ИББС-2.2-2009. «Методика оценки рисков нарушения информационной безопасности».
15. Что такое политика безопасности?
16. Что такое инженерная защита объектов?
17. Биометрия. Биометрические характеристики.
18. Что такое технические каналы утечки информации?
19. Перечислите основные виды технических каналов утечки информации?
20. Что такое спецпроверка?
21. Что такое специсследование?
22. Что такое спецобследование?
23. Что такое программно-аппаратные средства защиты информации?

24. Какие механизмы реализуют программно-аппаратные средства защиты информации?

25. Какие компьютерные угрозы безопасности существуют?

26. Что такое сетевая разведка? Какие методы защиты против нее существуют?

27. Что такое инъекция? Какие виды инъекций существуют? Какие методы защиты против них существуют?

28. Что такое отказ в обслуживании? Какие методы защиты против него существуют?

29. Основные виды программных уязвимостей.

30. Что такое шифр? Какие виды шифров существуют?

31. Что такое симметричный шифр?

32. Какие симметричные шифры используются сейчас?

33. Что такое ассиметричный шифр? Какие ассиметричные шифры используются сейчас?

34. Принцип построения симметричных шифров.

35. Принцип построения ассиметричных шифров.

36. Стандартные шифры.

37. Поточные шифры.

Краткие методические указания

Собеседование проводится в устной форме во время последнего занятия по теме. Обучающемуся задается 2 случайных вопроса из списка вопросов. Обучающийся должен ответить на вопросы в течение 5 минут. Во время проведения собеседования использование литературы и других информационных ресурсов не допускается.

Шкала оценки

№	Баллы	Описание
4	32–40	Студент полностью ответил на заданные вопросы
3	24–31	Студент смог почти полностью ответить на заданные вопросы
2	15–23	Студент дал неполный ответ на вопросы, но смог передать основную суть вопроса
1	0–14	Студент не смог или фрагментарно ответил на заданные вопросы

5.2 Примеры заданий для выполнения практических работ

Тема 1. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности.

Тема 2. Использование криптографических средств защиты информации.

Тема 3. Реализация работы инфраструктуры открытых ключей.

Тема 4. Средства стеганографии для защиты информации.

Тема 5. Настройка безопасного сетевого соединения.

Тема 6. Антивирусные средства защиты информации.

Краткие методические указания

На выполнение одной практической работы отводится не более 3 двухчасовых занятий. После выполнения каждой практической работы студент должен представить отчет о ее выполнении, а также, по указаниям преподавателя, выполнить дополнительные практические задания по теме практической работы.

Шкала оценки

№	Баллы	Описание
5	32–40	Студент предоставляет отчет попрактической работе оформленный в строгом соответстви и с требованиями вуза. Демонстрирует ход выполнения задания, отвечает на вопросы по з аданию.
4	26–31	Студент предоставляет отчет попрактической работе оформленный в строгом соответстви и с требованиями вуза. Демонстрирует ход выполнения задания, но не отвечает на вопрос ы по заданию.
3	18–25	Студент предоставляет отчет попрактической работе оформленный в строгом соответстви и с требованиями вуза. Но не способен продемонстрировать ход выполнения задания, отв ечает на вопросы по заданию.

2	11–24	Студент предоставляет отчет попрактической работе оформленный с ошибками соответст вии с требованиями вуза. не демонстрирует ход выполнения задания, отвечает на вопросы по заданию с неточностями.
1	0–10	Студентом демонстрирует отчет, но не может рассказали ни о выполнении задания, ни от ветить на вопросы по нему. Либо отчет не предоставлен

5.3 Контрольный тест

1. К правовым методам, обеспечивающим информационную безопасность, относятся:

- **а)** Разработка аппаратных средств обеспечения правовых данных
- **б)** Разработка и установка во всех компьютерных правовых сетях журналов учета действий
- **в)** Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2. Основными источниками угроз информационной безопасности являются все указанные в списке:

- **а)** Хищение жестких дисков, подключение к сети, инсайдерство
- **б)** Перехват данных, хищение данных, изменение архитектуры системы
- **в)** Хищение данных, подкуп системных администраторов, нарушение регламента работы

3. Виды информационной безопасности:

- **а)** Персональная, корпоративная, государственная
- **б)** Клиентская, серверная, сетевая
- **в)** Локальная, глобальная, смешанная

4. Цели информационной безопасности – своевременное обнаружение, предупреждение:

- **а)** Несанкционированного доступа, воздействия в сети
- **б)** Инсайдерства в организации
- **в)** Чрезвычайных ситуаций

5. Основные объекты информационной безопасности:

- **а)** Компьютерные сети, базы данных
- **б)** Информационные системы, психологическое состояние пользователей
- **в)** Бизнес-ориентированные, коммерческие системы

6. Основными рисками информационной безопасности являются:

- **а)** Искажение, уменьшение объёма, перекодировка информации
- **б)** Техническое вмешательство, выведение из строя оборудования сети
- **в)** Потеря, искажение, утечка информации

7. К основным принципам обеспечения информационной безопасности относится:

- **а)** Экономической эффективности системы безопасности
- **б)** Многоплатформенной реализации системы

- **в)** Усиления защищённости всех звеньев системы

8. Основными субъектами информационной безопасности являются:

- **а)** Руководители, менеджеры, администраторы компаний
- **б)** Органы права, государства, бизнеса
- **в)** Сетевые базы данных, фаерволлы

9. К основным функциям системы безопасности можно отнести всё перечисленное:

- **а)** Установление регламента, аудит системы, выявление рисков
- **б)** Установка новых офисных приложений, смена хостинг-компании
- **в)** Внедрение аутентификации, проверка контактных данных пользователей

10. Принципом информационной безопасности является принцип недопущения:

- **а)** Неоправданных ограничений при работе в сети (системе)
- **б)** Рисков безопасности сети, системы
- **в)** Презумпции секретности

11. Принципом политики информационной безопасности является принцип:

- **а)** Невозможности миновать защитные средства сети (системы)
- **б)** Усиления основного звена сети, системы
- **в)** Полного блокирования доступа при риск-ситуациях

12. Принципом политики информационной безопасности является принцип:

- **а)** Усиления защищённости самого незащищённого звена сети (системы)
- **б)** Перехода в безопасное состояние работы сети, системы
- **в)** Полного доступа пользователей ко всем ресурсам сети, системы

13. Принципом политики информационной безопасности является принцип:

- **а)** Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- **б)** Одноуровневой защиты сети, системы
- **в)** Совместимых, однотипных программно-технических средств сети, системы

14. К основным типам средств воздействия на компьютерную сеть относится:

- **а)** Компьютерный сбой
- **б)** Логические закладки («мины»)
- **в)** Аварийное отключение питания

15. Когда получен спам по e-mail с приложённым файлом, следует:

- **а)** Прочитать приложение, если оно не содержит ничего ценного – удалить
- **б)** Сохранить приложение в папке «Спам», выяснить затем IP-адрес генератора спама
- **в)** Удалить письмо с приложением, не раскрывая (не читая) его

16. Принцип Кирхгофа:

- **а)** Секретность ключа определена секретностью открытого сообщения
- **б)** Секретность информации определена скоростью передачи данных
- **в)** Секретность закрытого сообщения определяется секретностью ключа

17. ЭЦП – это:

- **а)** Электронно-цифровой преобразователь
- **б)** Электронно-цифровая подпись
- **в)** Электронно-цифровой процессор

18. Наиболее распространены угрозы информационной безопасности корпоративной системы:

- **а)** Покупка нелицензионного ПО
- **б)** Ошибки эксплуатации и неумышленного изменения режима работы системы
- **в)** Сознательное внедрение сетевых вирусов

19. Наиболее распространены угрозы информационной безопасности сети:

- **а)** Распределённый доступ клиента, отказ оборудования
- **б)** Моральный износ сети, инсайдерство
- **в)** Сбой (отказ) оборудования, нелегальное копирование данных

20. Наиболее распространены средства воздействия на сеть офиса:

- **а)** Слабый трафик, информационный обман, вирусы в интернет
- **б)** Вирусы в сети, логические мины (закладки), информационный перехват
- **в)** Компьютерные сбои, изменение администрирования, топологии

21. Утечкой информации в системе называется ситуация, характеризуемая:

- **а)** Потерей данных в системе
- **б)** Изменением формы информации
- **в)** Изменением содержания информации

22. Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

- **а)** Целостность
- **б)** Доступность
- **в)** Актуальность

23. Угроза информационной системе (компьютерной сети) – это:

- **а)** Вероятное событие
- **б)** Детерминированное (всегда определённое) событие
- **в)** Периодически повторяющееся событие

24. Информация, которую следует защищать (по нормативам, правилам сети, системы), называется:

- **а)** Регламентированной

- **б)** Правовой
- **в)** Защищаемой

25. Разновидностями угроз безопасности (сети, системы) являются все перечисленные в списке:

- **а)** Программные, технические, организационные, технологические
- **б)** Серверные, клиентские, спутниковые, наземные
- **в)** Личные, корпоративные, социальные, национальные

26. Окончательно, ответственность за защищённость данных в компьютерной сети несёт:

- **а)** Владелец сети
- **б)** Администратор сети
- **в)** Пользователь сети

27. Политика безопасности в системе (сети) – это комплекс:

- **а)** Руководств, требований обеспечения необходимого уровня безопасности
- **б)** Инструкций, алгоритмов поведения пользователя в сети
- **в)** Норм информационного права, соблюдаемых в сети

28. Наиболее важным при реализации защитных мер политики безопасности является:

- **а)** Аудит, анализ затрат на проведение защитных мер
- **б)** Аудит, анализ безопасности
- **в)** Аудит, анализ уязвимостей, риск-ситуаций

Краткие методические указания

Перед решением тестов внимательно следует ознакомься с каждым вопросом и предлагаемыми вариантами ответов. Затем необходимо опираясь на теоретический материал, связанный с темой вопроса сопоставить его с приведёнными вариантами. Выбирается тот ответ, который точно отражает изложенные факты.

Шкала оценки

№	Баллы	Описание
2	1	Студент дал верный ответ на тестовый вопрос
1	0	Студент дал не верный ответ на тестовый вопрос