МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины (модуля)

ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМАХ ОБРАБОТКИ ДАННЫХ

Направление и направленность (профиль)
11.03.02 Инфокоммуникационные технологии и системы связи. Защищенная инфокоммуникационная инфраструктура

Год набора на ОПОП
2026

Форма обучения
очная

Владивосток 2026

Рабочая программа дисциплины (модуля) «Защита информации в системах обработки данных» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 11.03.02 Инфокоммуникационные технологии и системы связи (утв. приказом Минобрнауки России от 19.09.2017г. №930) 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):

Етчо С.А.

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	0000000000FE821F
Владелец	Шумик Е.Г.

1 Цель, планируемые результаты обучения по дисциплине (модулю)

Цель: Формирование у студентов компетенций, необходимых для выполнения проектных работ по созданию систем защиты информации (СЗИ) автоматизированных систем (АС), включая сбор и анализ исходных данных (нормативных, технических, эксплуатационных) и разработку структурных/схемотехнических компонентов защиты.

Задачи

Обучить методикам идентификации источников исходных данных (ФСТЭК, Минцифры, ГОСТ, внутренняя документация заказчика) для обоснования требований к защите.

Сформировать навыки анализа технического задания (ТЗ) и формирования раздела "Требования к системе защиты информации" в проектной документации.

Изучить регламентирующие документы, определяющие классы защищенности АС и уровни доверия к средствам защиты.

Освоить принципы проектирования подсистем: управления доступом, криптографической защиты, антивирусной защиты, обнаружения вторжений (IDS/IPS), межсетевого экранирования.

Сформировать практические навыки расчета показателей защищенности (вероятность взлома, время восстановления) на этапе проектирования.

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	
11.03.02 «Инфокоммуникационные технологии и системы связи» (Б-ИК)	ПКВ-4 : Способен осуществлять сбор и анализ исходных данных для проектирования, проектировать и разрабатывать устройства связи и компоненты систем защиты информации	ПКВ-4.1к : Определяет источники информации, регламентирующие деятельность, связанную с организацией политики безопасности	РД1	Знание	Состав и иерархию нормативных правовых актов, регламентирующих защиту информации в РФ; перечень исходных данных, необходимых для проектирования СЗИ (класс АС, категория обрабатываемой информации, модель угроз)
			РД2	Умение	Собирать и анализировать техническую документацию на объект защиты; формулировать требования к системе защиты на основе анализа регламентов.

			РД3	Навык	составления технического задания (ТЗ) на проектирование СЗИ и оформления раздела "Политика безопасности" в проектной документации.
		ПКВ-4.2к : Разрабатывает компоненты комплексных систем защиты информации автоматизированных систем	РД4	Знание	Типовые архитектуры компонентов СЗИ (межсетевые экраны, средства криптозащиты, СОВ, подсистемы аудита); методы сопряжения аппаратных и программных модулей защиты.
			РД4	Умение	Проектировать конфигурации средств защиты под конкретную топологию АС; обосновывать выбор компонентов (отечественных или импортных) по критериям стоимости и эффективности.
			РД6	Навык	разработки структурных, функциональных и принципиальных схем компонентов СЗИ; методиками проверки работоспособности спроектированных узлов.

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	Осознание ценности профессии
Формирование духовно-нравственных ценностей		

Формирование ответственного отношения к труду	Служение Отечеству и ответственность за его судьбу	Коммуникабельность
Формирование научного мировоззрения и культуры мышления		
Развитие познавательного интереса и стремления к знаниям	Взаимопомощь и взаимоуважение	Ответственность
Формирование коммуникативных навыков и культуры общения		
Воспитание культуры диалога и уважения к мнению других людей	Коллективизм	Внимательность к деталям

2 Место дисциплины (модуля) в структуре ОПОП

дисциплина относится к вариативной части учебного плана и опирается на следующий дисциплины "Основы информационной безопасности", "Информатика и основы программирования" и необходима для изучения следующих дисциплин: "Организационное и правовое обеспечение информационной безопасности", "Мониторинг событий и управление инцидентами"

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 обучения	Часть УП	Семестр (ОФО) или курс (ЗФО, ОЗФО)	Трудоемкость	Объем контактной работы (час)						СРС	Форма аттестации
				(З.Е.)	Всего	Аудиторная			Внеаудиторная			
						лек.	прак.	лаб.	ПА	КСР		
11.03.02 Инфокоммуникационные технологии и системы связи	ОФО	Б1.В	3	5	55	18	36	0	1	0	125	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 результата обучения	Кол-во часов, отведенное на				Форма текущего контроля
			Лек	Практ	Лаб	СРС	

1	Нормативно-правовая база и сбор исходных данных	РД1, РД2	2	6	0	30	практическое задание, тест
2	Архитектура и компоненты СЗИ	РД4, РД4, РД6	6	10	0	32	практическое задание, тест
3	Проектирование систем мониторинга и анализа защищенности	РД4, РД4, РД6	4	10	0	32	практическое задание, тест
4	Проектная документация и оценка системы защиты	РД2, РД3	6	10	0	32	практическое задание, тест
Итого по таблице			**18**	**36**	**0**	**126**	

4.2 Содержание разделов и тем дисциплины (модуля) для ОФО

Тема 1 Нормативно-правовая база и сбор исходных данных.

Содержание темы: Иерархия регламентирующих документов. Федеральные законы (№149-ФЗ, №152-ФЗ, №187-ФЗ), Приказы ФСТЭК (№31, №17, №239), ГОСТы серии 34, стандарты Банка России. Разграничение требований для ГИС, ИСПДн, АСУ ТП, КИИ. Анализ исходных данных для проектирования. Определение класса защищенности АС (по методике ФСТЭК). Анализ модели угроз безопасности информации (приказ ФСТЭК №31). Оценка категорий обрабатываемых данных и критичности информационных ресурсов. Формирование ТЗ на СЗИ. Структура раздела "Требования к системе защиты" в ТЗ. Методика согласования проектных решений с заказчиком и регуляторами.

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

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 2 Архитектура и компоненты СЗИ.

Содержание темы: Подсистема управления доступом и регистрации. Проектирование политик разграничения доступа на основе дискреционных, мандатных и ролевых моделей. Разработка схемы потоков информации в АС. Средства криптографической защиты (СКЗИ). Выбор и обоснование использования СКЗИ (класс КС1, КС2, КС3). Проектирование узлов криптошлюзов и защищенных VPN-туннелей. Управление ключевой системой на этапе проектирования. Активные средства защиты (СЗИ от НСД, антивирусы, МЭ). Проектирование подсетей DMZ. Разработка правил фильтрации для межсетевого экрана. Обоснование выбора антивирусных комплексов и систем обнаружения вторжений (IDS/IPS) для узлов сегмента СОД.

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

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 3 Проектирование систем мониторинга и анализа защищенности.

Содержание темы: Системы сбора и корреляции событий (SIEM). Проектирование архитектуры сбора логов с различных узлов СОД. Определение перечня регистрируемых событий в соответствии с требованиями регуляторов. Резервирование и отказоустойчивость компонентов защиты. Расчет надежности СЗИ. Методы горячего/холодного резервирования критичных элементов защиты (криптосерверы, прокси). Инженерно-техническая защита. Разработка схем экранирования помещений (клетка Фарадея) и организации защищенных каналов связи на физическом уровне.

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

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 4 Проектная документация и оценка системы защиты.

Содержание темы: Оформление рабочей документации. Состав и содержание разделов проектной документации. Спецификации оборудования и кабельных трасс. Расчет количественных показателей защищенности (вероятность парирования угроз, время реакции системы). Проведение контрольных тестов спроектированной СЗИ.

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

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

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, которую они совершают без непосредственной помощи и указаний преподавателя, руководствуясь сформировавшимися ранее представлениями о порядке и правильности выполнения операций. Цель СРС в процессе обучения заключается, как в усвоении знаний, так и в формировании умений и навыков по их использованию в новых условиях на новом учебном материале. Самостоятельная работа призвана обеспечивать возможность осуществления студентами самостоятельной познавательной деятельности в обучении, и является видом учебного труда, способствующего формированию у студентов самостоятельности. В данной учебной программе приведен перечень основных и дополнительных источников, которые предлагается изучить в процессе облучения по дисциплине. Кроме того, для расширения 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 бумажных носителях. Успешное освоение дисциплины предполагает активную работу студентов на всех занятиях аудиторной формы: лекций и практических занятий, выполнение аттестационный мероприятий, эффективную самостоятельную работу. В процессе изучения дисциплины студенту необходимо ориентироваться на самостоятельную проработку лекционного материала, подготовку к практическим занятиям, выполнение тестов, кейсовых заданий, самостоятельное изучение некоторых разделов курса Для проведения занятий лекционного типа используются учебно-наглядные пособия в форме презентационных материалов, обеспечивающих тематические иллюстрации, соответствующие темам лекций, представленным в пункте 4 настоящей РПД.

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. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2026. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/584673 (дата обращения: 19.05.2026).

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. Основы криптографии : учебное пособие / составители И. А. Кривошеев, А. В. Попова. — Хабаровск : ДВГУПС, 2025. — 99 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/519328 (дата обращения: 25.05.2026). — Режим доступа: для авториз. пользователей.

7.2 Дополнительная литература

1. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2026. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2238628 (дата обращения: 31.05.2026)

2. Сергеева, О. А. Основы криптографии : учебно-методическое пособие / О. А. Сергеева, А. С. Кутовая. — Кемерово : КемГУ, 2024. — 160 с. — ISBN 978-5-8353-3120-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/407729 (дата обращения: 25.05.2026). — Режим доступа: для авториз. пользователей.

3. СПС Консультант Плюс

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

1. Образовательная платформа "ЮРАЙТ"
2. Электронно-библиотечная система "ZNANIUM.COM"
3. Электронно-библиотечная система "ЛАНЬ"
4. Open Academic Journals Index (OAJI). Профессиональная база данных - Режим доступа: http://oaji.net/
5. 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

Программное обеспечение:

- Microsoft Office Professional Plus 2010

МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМАХ ОБРАБОТКИ ДАННЫХ

Направление и направленность (профиль)
11.03.02 Инфокоммуникационные технологии и системы связи. Защищенная инфокоммуникационная инфраструктура

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
11.03.02 «Инфокоммуникационные технологии и системы связи» (Б-ИК)	ПКВ-4 : Способен осуществлять сбор и анализ исходных данных для проектирования, проектировать и разрабатывать устройства связи и компоненты систем защиты информации	ПКВ-4.1к : Определяет источники информации, регламентирующие деятельность, связанную с организацией политики безопасности
		ПКВ-4.2к : Разрабатывает компоненты комплексных систем защиты информации автоматизированных систем

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 ПКВ-4 «Способен осуществлять сбор и анализ исходных данных для проектирования, проектировать и разрабатывать устройства связи и компоненты систем защиты информации»

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	
ПКВ-4.1к : Определяет источники информации, регламентирующие деятельность, связанную с организацией политики безопасности	РД 1	Знание	Состав и иерархию нормативных правовых актов, регламентирующих защиту информации в РФ; перечень исходных данных, необходимых для проектирования СЗИ (класс АС, категория обрабатываемой информации, модель угроз)	тест
	РД 2	Умение	Собирать и анализировать техническую документацию на объект защиты; формулировать требования к системе защиты на основе анализа регламентов.	практическая работа
	РД 3	Навык	составления технического задания (ТЗ) на проектирование СЗИ и оформления раздела " Политика безопасности" в проектной документации.	выполнение практических заданий
ПКВ-4.2к : Разрабатывает компоненты комплексных систем защиты информации автоматизированных систем	РД 4	Знание	Типовые архитектуры компонентов СЗИ (межсетевые экраны, средства криптозащиты, СОВ, подсистемы аудита); методы сопряжения аппаратных	тест

			и программных модулей защиты.	
	РД 4	Умение	Проектировать конфигурации средств защиты под конкретную топологию АС; обосновывать выбор компонентов (отечественных или импортных) по критериям стоимости и эффективности.	выполнение практических заданий
	РД 6	Навык	разработки структурных, функциональных и принципиальных схем компонентов СЗИ; методиками проверки работоспособности спроектированных узлов.	выполнение практических заданий

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 : Состав и иерархию нормативных правовых актов, регламентирующих защиту информации в РФ; перечень исходных данных, необходимых для проектирования СЗИ (класс АС, категория обрабатываемой информации, модель угроз)	1.1. Нормативно-правовая база и сбор исходных данных	Тест	Экзамен в устной форме
РД2	Умение : Собирать и анализировать техническую документацию на объект защиты; формулировать требования к системе защиты на основе анализа регламентов.	1.1. Нормативно-правовая база и сбор исходных данных	Практическая работа	Экзамен в устной форме
		1.4. Проектная документация и оценка системы защиты	Практическая работа	Экзамен в устной форме
РД3	Навык : составления технического задания (ТЗ) на проектирование СЗИ и оформления раздела " Политика безопасности" в проектной документации.	1.4. Проектная документация и оценка системы защиты	Практическая работа	Экзамен в устной форме
РД4	Знание : Типовые архитектуры компонентов СЗ	1.2. Архитектура и компоненты СЗИ	Тест	Экзамен в устной форме

	И (межсетевые экраны, средства криптозащиты, СОВ, подсистемы аудита); методы сопряжения аппаратных и программных модулей защиты.	1.3. Проектирование систем мониторинга и анализа защищенности	Тест	Экзамен в устной форме
РД4	Умение : Проектировать конфигурации средств защиты под конкретную топологию АС; обосновывать выбор компонентов (отечественных или импортных) по критериям стоимости и эффективности.	1.2. Архитектура и компоненты СЗИ	Практическая работа	Экзамен в устной форме
		1.3. Проектирование систем мониторинга и анализа защищенности	Практическая работа	Экзамен в устной форме
РД6	Навык : разработки структурных, функциональных и принципиальных схем компонентов СЗИ; методиками проверки работоспособности спроектированных узлов.	1.2. Архитектура и компоненты СЗИ	Практическая работа	Экзамен в устной форме
		1.3. Проектирование систем мониторинга и анализа защищенности	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 1-5	Практическая работа	Экзамен	Итого
Лекционные занятия	20			20
Практические занятия		60		60
Промежуточная аттестация			20	20
Итого	20	60	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 Контрольный тест

Вопрос 1

Каким основным нормативным документом регламентируется порядок определения класса защищенности автоматизированной системы (АС) в РФ?

А) ГОСТ Р ИСО/МЭК 27001

Б) Приказ ФСТЭК России от 14.03.2014 № 31 (ред. от 2021 г.)

В) Федеральный закон № 149-ФЗ «Об информации...»

Г) Методика ФСТЭК по оценке угроз от 05.02.2021

Вопрос 2

Что из перечисленного является исходными данными, необходимыми для начала проектирования системы защиты информации (СЗИ)?

А) Цена лицензии на антивирусное ПО

Б) Модель угроз безопасности информации и категория обрабатываемых данных

В) Список сотрудников отдела информатизации

Г) Максимальная пропускная способность канала связи

Вопрос 3

Какой документ в первую очередь подлежит анализу при сборе исходных данных для проектирования СЗИ объекта КИИ (критической информационной инфраструктуры)?

А) Устав предприятия

Б) Требования Приказа Минцифры по аттестации объектов КИИ

В) Инструкция по делопроизводству

Г) Правила внутреннего трудового распорядка

Вопрос 4

На этапе разработки структурной схемы компонента СЗИ (криптошлюза) инженер должен в первую очередь определить:

А) Дизайн интерфейса администрирования

Б) Место включения устройства в топологию сети и способы маршрутизации защищённого трафика

В) Цвет корпуса оборудования

Г) Версию операционной системы рабочей станции разработчика

Вопрос 5

Какой параметр является критическим при обосновании выбора межсетевого экрана (МЭ) для сегмента СОД с высокой нагрузкой (более 10 Гбит/с)?

А) Наличие графического интерфейса

Б) Производительность по пропускной способности (Throughput) с включенными правилами фильтрации

В) Количество портов USB на корпусе

Г) Вес оборудования

Вопрос 6

В соответствии с требованиями по разработке компонентов СЗИ, что из перечисленного относится к подсистеме регистрации и аудита?

А) Настройка правил трансляции адресов (NAT)

Б) Фиксация всех событий входа/выхода пользователей и изменения прав доступа

В) Сканирование входящей почты на вирусы

Г) Шифрование трафика между серверами

Вопрос 7

При анализе модели угроз (Приказ ФСТЭК №31) для проектирования СЗИ, какой пункт должен быть учтён в первую очередь?

А) Наличие резервного источника питания

Б) Степень квалификации возможного нарушителя и его положение (внутренний/внешний)

В) Количество серверов в стойке

Г) Срок гарантии на оборудование

Вопрос 8

Как правильно спроектировать размещение системы обнаружения вторжений (IDS) в защищенной СОД?

А) Установить только на рабочей станции бухгалтера

Б) Установить в режиме «зеркалирования порта» (SPAN) на ключевом сетевом коммутаторе для анализа всего трафика сегмента

В) Установить вместо межсетевого экрана

Г) Установить на шлюзе в разрыв линии (inline), блокируя весь трафик

Вопрос 9

Что является источником информации, регламентирующим деятельность по организации политики безопасности для ИСПДн (информационные системы персональных данных) 1-го уровня защищенности?

А) СанПиН

Б) Приказ ФСТЭК № 17 и Постановление Правительства РФ № 1119

В) ГОСТ Р 34.10

Г) Трудовой кодекс РФ

Вопрос 10

В проекте СЗИ для распределенной СОД предлагается использовать два центра сертификации (УЦ) и резервный криптошлюз. Данное решение относится к проектированию:

А) Подсистемы криптографической защиты с отказоустойчивостью (High Availability)

Б) Подсистемы физической защиты периметра

В) Модуля антивирусной очистки

Г) Системы кондиционирования воздуха в ЦОД

Краткие методические указания

Тестовые задания состоят из вопроса и нескольких вариантов ответа. Решение представляет собой указание номера вопроса и букву, которой обозначен правильный, по мнению студента, вариант ответа. В течение семестра проводится 4 теста по 4 темам на лекционных занятиях, в каждом тесте 16 вопросов.

Шкала оценки

Оценка	Баллы	Описание
5	5	Студент допустил не более 2х ошибок
4	4	Студент совершил от 3 до 6 ошибок в ответах на тест
3	2-3	Студент совершил от 7 до 10 ошибок в ответах на тест
2	0-1	Студент совершил 11 и более ошибок в ответах на тест

5.2 Примеры заданий для выполнения практических работ

Практическая работа № 1 (ПКВ-4.1к)

Цель: Сформировать навыки анализа технического задания (ТЗ) заказчика, идентификации регламентирующих документов и определения класса защищенности автоматизированной системы (АС).

Задание 1. Анализ вводной информации

Вам предоставлено ТЗ заказчика (выдержка):

«Объект автоматизации — корпоративная информационная система обработки персональных данных (ИСПДн) сотрудников и клиентов. Количество субъектов ПДн —

более 100 000. Обрабатываются специальные категории ПДн (состояние здоровья). Система имеет подключение к сети Интернет для обмена данными с контрагентами. Требуется обеспечить защиту в соответствии с законодательством РФ.»

Вопросы для анализа (письменный ответ):

Определите категорию обрабатываемых персональных данных согласно Постановлению Правительства РФ № 1119.

Какой уровень защищенности ПДн должен быть присвоен данной ИС? Обоснуйте.

Перечислите не менее 3-х нормативных документов, которые являются источниками исходных данных для проектирования СЗИ в данной системе (укажите полные названия и реквизиты).

Какие дополнительные исходные данные необходимо запросить у заказчика для полноценного проектирования (не менее 4-х позиций)?

Задание 2. Формирование требований к СЗИ

На основе проанализированных исходных данных составьте фрагмент раздела «Требования к системе защиты информации» для ТЗ (объем — не менее 10 пунктов), включив требования к:

Средствам криптографической защиты (СКЗИ);

Средствам антивирусной защиты;

Системе разграничения доступа;

Регистрации и учёту событий безопасности.

Задание 3. Заполнение карты исходных данных

Заполните таблицу (шаблон):

Наименование параметра Значение / Ссылка на документ

Класс защищенности АС (по Приказу ФСТЭК №31)

Уровень защищенности ПДн (Постановление №1119)

Категория объекта КИИ (если применимо)

Базовая модель угроз (реквизиты документа)

Перечень защищаемой информации (грифы)

Требования к СКЗИ (класс, уровень)

Форма отчета: Письменный отчет в формате служебной записки с обоснованием каждого выбора.

Практическая работа № 2

Цель: Получить навыки проектирования компонентов криптографической защиты с обоснованием выбора оборудования и места его включения в сетевую архитектуру.

Задание 1. Анализ архитектуры объекта

Дана топология распределенной системы обработки данных:

Центральный офис (ЦО): серверная ферма (СУБД, файловый сервер, сервер приложений), 50 рабочих станций, выход в Интернет.

2 удаленных филиала (РФ): по 20 рабочих станций, подключение к ЦО через публичные каналы связи (провайдер).

Требуется организовать защищенный обмен данными между филиалами и ЦО с обеспечением конфиденциальности и целостности, а также защиту сегмента серверов от внешних атак.

Задание 2. Выбор компонентов СЗИ

Обоснуйте выбор следующего оборудования/ПО для данного объекта (предложите конкретные наименования и их функции):

Средство криптографической защиты (СКЗИ) для организации VPN-туннелей.

Межсетевой экран (МЭ) для защиты периметра ЦО.

Система обнаружения вторжений (IDS) для контроля трафика внутри сегмента СОД.

Для каждого выбора укажите:

Функциональное назначение в составе СЗИ.

Место включения в топологию (сетевой адрес, интерфейс, сетевая зона).

Обоснование (почему именно это средство, ссылка на требования нормативных документов, если есть).

Задание 3. Разработка структурной схемы

Используя условные графические обозначения (можно вручную, в Visio или любом другом редакторе), разработайте структурную схему СЗИ для данной распределенной СОД, где должны быть отражены:

Все узлы сети (ЦО и филиалы);

Места установки межсетевых экранов;

VPN-шлюзы (криптошлюзы) с указанием шифрованных туннелей;

Сегментация сетей (DMZ, внутренняя сеть);

Серверы сбора событий (при необходимости).

К схеме приложите текстовое описание (легенду) со спецификацией компонентов.

Задание 4. Расчет пропускной способности криптошлюза

Исходные данные:

В ЦО средний трафик к филиалу — 500 Мбит/с (в пике до 1 Гбит/с).

Выбранное СКЗИ имеет производительность 800 Мбит/с при шифровании AES-256.

Вопрос: Выдержит ли выбранное средство пиковую нагрузку? Если нет, предложите проектное решение (кластеризация, балансировка нагрузки) с обоснованием.

Форма отчета: Пояснительная записка с приложением схемы и спецификации.

Практическая работа № 3

Цель: Интегрировать навыки разработки политик безопасности (нормативный аспект) и их технической реализации на конкретном оборудовании (проектный аспект).

Этап 1. Разработка политики безопасности

Для гипотетической АС, обрабатывающей персональные данные, разработайте фрагмент Политики безопасности, включающий:

Правила разграничения доступа для 3 типов пользователей: администратор, оператор, аудитор.

Регламент смены паролей и требования к их сложности (со ссылкой на Приказ ФСТЭК).

Перечень регистрируемых событий (не менее 10) с указанием периодичности их проверки.

Порядок реагирования на инцидент (краткая блок-схема).

Этап 2. Настройка межсетевого экрана— расчетно-графическая часть

Вам дана сеть: 192.168.1.0/24 — внутренняя сеть СОД (серверы), 192.168.2.0/24 — сеть пользователей, 10.0.0.0/30 — внешний канал (провайдер).

Разработайте набор правил фильтрации для межсетевого экрана (в виде таблицы) со следующими политиками:

№ Действие (Allow/Deny) Источник Назначение Протокол/Порт Комментарий (обоснование)

1 Allow Администратор (192.168.2.10) Сервер СУБД (192.168.1.5) TCP 1433 Управление БД (по ТЗ)

2 Deny Все Сервер СУБД (192.168.1.5) TCP 1433 Запрет доступа для всех, кроме админов

3 ... ...

Составьте не менее 10 правил, охватывающих:

Доступ к корпоративному веб-серверу из внешней сети;

Запрет доступа к внутренней сети СОД из сегмента пользователей (кроме разрешённых);

Разрешение доступа к DNS и NTP для всех узлов;

Логирование всех попыток доступа из внешней сети к закрытым ресурсам.

Этап 3. Конфигурирование системы регистрации событий

Разработайте шаблон настройки сбора событий для одного узла (например, сервер СУБД), указав:

Какие системные журналы (логи) должны собираться (аудит входа, изменения прав, запуск/остановка служб);

Куда должны отправляться события (IP-адрес SIEM-сервера);

Частота отправки (в реальном времени / каждые 5 минут);

Требования к защите канала передачи событий от перехвата и подмены.

Этап 4. Анализ соответствия требованиям

Проверьте спроектированные правила и конфигурации на соответствие одному из нормативных документов (например, Приказу ФСТЭК №17 для ИСПДн). Напишите краткое заключение, какие требования выполнены, а какие требуют доработки.

Краткие методические указания

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

Шкала оценки

Оценка	Баллы	Описание
5	8-10	Оценка «отлично» выставляется, если студент выполнил задание, правильно применил методы.
4	5-7	Оценка «хорошо» выставляется, если студент выполнил задание, правильно применил методы, но совершил логические ошибки.
3	2-4	Оценка «удовлетворительно» выставляется, если студент выполнил задание, но применил методы не все необходимые методы для его выполнения.
2	0-1	Оценка «неудовлетворительно» выставляется в случае, если студент не выполнил задание и/ или неверно применил методы необходимые его выполнения.

5.3 Вопросы к экзамену

Вопрос 1

Опишите полную иерархию нормативных правовых актов Российской Федерации, регламентирующих защиту информации в автоматизированных системах.

Начиная с федеральных законов, укажите:

- какие документы определяют общие требования к защите информации;
- какие документы устанавливают конкретные требования к защите персональных данных, государственной тайны, объектов КИИ;
- какие документы определяют правила классификации АС и оценки угроз.

Для каждого уровня иерархии приведите конкретные примеры документов с полными названиями и реквизитами.

Вопрос 2

Разработайте алгоритм (пошаговую методику) сбора и анализа исходных данных для проектирования системы защиты информации (СЗИ) вновь создаваемой автоматизированной системы, обрабатывающей персональные данные 2-го уровня защищенности. Опишите:

- какие исходные данные необходимо запросить у заказчика;
- какие нормативные документы подлежат анализу;
- в каком порядке выполняются этапы (обследование, классификация, анализ угроз, формирование требований);
- какой документ является итоговым результатом сбора исходных данных.

Вопрос 3

Сравните требования к защите информации для трёх типов систем:

- Государственная информационная система (ГИС) 1-го класса;
- Информационная система персональных данных (ИСПДн) 1-го уровня защищенности;

- Объект критической информационной инфраструктуры (КИИ) 1-й категории значимости.

Для каждого типа укажите:

- регламентирующие документы (не менее 2-х для каждого);
- обязательный состав организационных и технических мер защиты;
- требования к сертификации/аттестации.

Вопрос 4

Спроектируйте подсистему криптографической защиты (СКЗИ) для распределенной системы обработки данных со следующей архитектурой:

- Центральный офис (ЦО): 100 рабочих станций, серверная ферма (СУБД, файловый сервер, веб-сервер);
- 4 удаленных филиала по 15-20 рабочих станций;
- Связь между филиалами и ЦО осуществляется через открытые каналы Интернет;
- Требуется обеспечить конфиденциальность и целостность всего трафика между узлами.

Вопрос 5

Разработайте проектное решение по защите серверного сегмента СОД от несанкционированного доступа и внешних атак с использованием межсетевого экрана (МЭ) и системы обнаружения вторжений (IDS).

Вопрос 6

Спроектируйте подсистему управления доступом и регистрации событий для автоматизированной системы с ролевой структурой пользователей:

- Администратор безопасности — полный доступ ко всем ресурсам;
- Администратор СОД — доступ к настройке серверов, но без доступа к журналам безопасности;
- Оператор — доступ только к своим данным (дискреционная модель на уровне записей в БД);
- Аудитор — доступ на чтение всех журналов, но без права изменения конфигурации.

Вопрос 7

Дано техническое задание заказчика на проектирование СЗИ для корпоративной системы обработки данных:

«Объект защиты — информационная система коммерческой организации, обрабатывающая:

— персональные данные сотрудников (2000 записей);
— сведения о контрагентах, составляющие коммерческую тайну;
— финансовую отчётность.

Система состоит из центрального офиса (50 АРМ) и 2-х небольших филиалов (по 10 АРМ), подключённых к центральному офису через Интернет с использованием VPN (используется встроенное средство ОС). В центральном офисе функционируют 5 серверов (файловый, почтовый, 1С, СУБД, веб-сервер для внешних клиентов). В штате организации нет выделенного администратора безопасности — обязанности распределены между системными администраторами.»

Вопрос 8

Разработайте архитектуру системы сбора и корреляции событий (SIEM) для крупной распределённой СОД, состоящей из:

- центрального офиса (200 узлов);
- 10 региональных офисов (по 30-50 узлов каждый);
- облачной инфраструктуры (виртуальные машины в AWS/Yandex Cloud).

Вопрос 9

Разработайте проектную документацию (фрагменты) для компонента СЗИ — защищённого VPN-шлюза на основе отечественной ОС (Astra Linux Special Edition) и СКЗИ (КриптоПро или VipNet). В ответе необходимо:

1. Обосновать выбор ОС и СКЗИ (ссылки на реестр отечественного ПО, сертификаты ФСТЭК/ФСБ).

2. Разработать структурную схему включения VPN-шлюза в сетевую топологию СОД.

3. Составить спецификацию оборудования и ПО для данного компонента.

4. Разработать фрагмент инструкции администратора по первоначальной настройке VPN-шлюза (базовые шаги).

5. Указать, какие разделы проектной документации стадии «РД» должны содержать сведения о данном компоненте.

Вопрос 10

Полный цикл проектирования СЗИ для системы обработки данных медицинской организации, обрабатывающей специальные категории персональных данных (сведения о состоянии здоровья). В ответе необходимо последовательно раскрыть все этапы

Краткие методические указания

Для подготовки к экзамену студенту необходимо изучить лекционный материал, а так же материал представленный в дополнительных источниках.

Шкала оценки

Оценка	Баллы	Описание
5	14-20	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал исчерпывающе, последовательно, четко и логически стройно его излагает , умеет тесно увязывать теорию с практикой.
4	8-12	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач.
3	2-6	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки.
2	0-2	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки.