МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
"САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ"

Кафедра № 33

УТВЕРЖДАЮ
Руководитель образовательной программы

доц.,к.э.н.,доц.
(должность, уч. степень, звание)

Т.Н. Елина
(инициалы, фамилия)

(подпись)
«20» февраля 2026 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Методология защиты информации»
(Наименование дисциплины)

Код направления подготовки/ специальности	10.03.01
Наименование направления подготовки/ специальности	Информационная безопасность
Наименование направленности/ специализации	Безопасность компьютерных систем
Форма обучения	очная
Год приема	2026

Санкт-Петербург– 2026

Лист согласования рабочей программы дисциплины

Программу составил (а)

доц.,к.э.н.,доц. — 20.02.26 — Т.Н. Елина
(должность, уч. степень, звание) (подпись, дата) (инициалы, фамилия)

Программа одобрена на заседании кафедры № 33
«20» февраля 2026 г, протокол № 7

Заведующий кафедрой № 33
д.т.н.,проф. — 20.02.26 — С.В. Беззатеев
(уч. степень, звание) (подпись, дата) (инициалы, фамилия)

Заместитель директора института №3 по методической работе
доц.,к.т.н. — 20.02.26 — Н.В. Решетникова
(должность, уч. степень, звание) (подпись, дата) (инициалы, фамилия)

Аннотация

Дисциплина «Методология защиты информации» входит в образовательную программу высшего образования – программу бакалавриата по направлению подготовки/ специальности 10.03.01 «Информационная безопасность» направленности/специализации «Безопасность компьютерных систем». Дисциплина реализуется кафедрой «№33».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ПК-3 «Способен применять современные теоретические и экспериментальные методы исследования с целью создания новых перспективных средств защиты информации, способен к использованию и внедрению результатов исследований»

ПК-6 «Способен администрировать средства защиты информации прикладного и системного программного обеспечения»

Содержание дисциплины охватывает круг вопросов, связанных с изучением методов, теоретических и практических основ обеспечения информационной безопасности в автоматизированных информационных системах.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные работы, самостоятельная работа студента.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме зачета (7 семестр).

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа.

Язык обучения по дисциплине «русский »

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Цель преподавания дисциплины – изучение методов, теоретических и практических основ обеспечения информационной безопасности в автоматизированных информационных системах.

1.2. Дисциплина входит в состав части, формируемой участниками образовательных отношений, образовательной программы высшего образования (далее – ОП ВО).

1.3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОП ВО.

В результате изучения дисциплины обучающийся должен обладать следующими компетенциями или их частями. Компетенции и индикаторы их достижения приведены в таблице 1.

Таблица 1 – Перечень компетенций и индикаторов их достижения

Категория (группа) компетенции	Код и наименование компетенции	Код и наименование индикатора достижения компетенции
Профессиональные компетенции	ПК-3 Способен применять современные теоретические и экспериментальные методы исследования с целью создания новых перспективных средств защиты информации, способен к использованию и внедрению результатов исследований	ПК-3.З.1 знает методы и средства планирования и организации исследований и разработок ПК-3.З.2 знает методы анализа научных данных ПК-3.У.1 умеет применять актуальную нормативную документацию в соответствующей области знаний ПК-3.У.2 умеет оформлять результаты научно-исследовательских и опытно-конструкторских работ ПК-3.В.1 владеет навыками организации сбора и изучения научно-технической информации по теме исследований и разработок ПК-3.В.2 владеет навыками анализа научных данных, результатов экспериментов и наблюдений
Профессиональные компетенции	ПК-6 Способен администрировать средства защиты информации прикладного и системного программного обеспечения	ПК-6.З.1 знает уязвимости используемого программного обеспечения и методы их эксплуатации

2. Место дисциплины в структуре ОП

Дисциплина может базироваться на знаниях, ранее приобретенных обучающимися при изучении следующих дисциплин:

– «Основы информационной безопасности»,
– «Основы проектной деятельности в профессии»,
– «Информатика».

Знания, полученные при изучении материала данной дисциплины, имеют как самостоятельное значение, так и используются при изучении других дисциплин:

– «Основы управления информационной безопасностью»,

– «Научно-исследовательская работа».

3. Объем и трудоемкость дисциплины

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 2.

Таблица 2 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№7
1	2	3
Общая трудоемкость дисциплины, ЗЕ/ (час)	2/ 72	2/ 72
Из них часов практической подготовки	17	17
Аудиторные занятия, всего час.	34	34
в том числе:		
лекции (Л), (час)	17	17
практические/семинарские занятия (ПЗ), (час)		
лабораторные работы (ЛР), (час)	17	17
курсовой проект (работа) (КП, КР), (час)		
экзамен, (час)		
Самостоятельная работа, всего (час)	38	38
***Вид промежуточной аттестации*:** зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.)	Зачет,	Зачет,

4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий.

Разделы, темы дисциплины и их трудоемкость приведены в таблице 3.

Таблица 3 – Разделы, темы дисциплины, их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП/КР (час)	СР (час)
Семестр 7					
1. Методы анализа рисков информационной безопасности	4		3		6
2. Информационные активы предприятия	2		2		6
3. Методика COBIT: назначение, правила использования	2		2		6
4. Система поддержки принятия парето-оптимальных решений в области проектирования системы защиты информации на предприятии	2		2		6
5. Анализ и оценка рисков информационной безопасности с использованием нечеткой логики	4		4		6
6. Определение показателей защищенности информации при несанкционированном доступе	5		4		8
Итого в семестре:	17		17		38

Итого	17	0	17	0	38

Практическая подготовка заключается в непосредственном выполнении обучающимися определенных трудовых функций, связанных с будущей профессиональной деятельностью.

4.2. Содержание разделов и тем лекционных занятий.

Содержание разделов и тем лекционных занятий приведено в таблице 4.

Таблица 4 – Содержание разделов и тем лекционного цикла

Номер раздела	Название и содержание разделов и тем лекционных занятий
1	Методы анализа рисков информационной безопасности 1. Введение в анализ рисков ИБ • Определение понятий: Актив, угроза, уязвимость, риск, вероятность, ущерб. • Цели и задачи анализа рисков: Определение приемлемого уровня риска, выбор мер защиты. • Этапы управления рисками: Идентификация, оценка, обработка, мониторинг. 2. Классификация методов анализа рисков • Качественные методы (Qualitative): Основаны на экспертных оценках, ранжировании (высокий/средний/низкий). • Количественные методы (Quantitative): Основаны на числовых данных, расчете вероятности и финансового ущерба. • Смешанные (гибридные) методы: Сочетание экспертной оценки с расчетами. 3. Основные подходы и методологии • Метод на основе активов (Asset-based): Фокус на критичности информационных активов. • Метод на основе угроз (Threat-based): Анализ наиболее вероятных сценариев атак. • Метод на основе уязвимостей (Vulnerability-based): Анализ слабых мест инфраструктуры. 4. Стандартизированные методики • ISO/IEC 27005: Общие принципы управления рисками ИБ. • NIST SP 800-30: Методология оценки рисков. • OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation): Методика самооценки. • CRAMM (CCTA Risk Analysis and Management Method): Структурированный качественный/количественный метод. 5. Инструментарий и документирование • Автоматизированные средства: Использование специализированного ПО (GRC-системы). • Оформление результатов: Составление реестра рисков, карты рисков (Risk Map) и отчета
2	2. Информационные активы предприятия Классификация и идентификация: • Данные: базы данных, клиентские реестры, финансовая отчетность, интеллектуальная собственность. • Программное обеспечение: прикладные программы, операционные

	системы, лицензии. • Аппаратное обеспечение: серверы, рабочие станции, сетевое оборудование. Управление жизненным циклом: • Планирование, приобретение/разработка, эксплуатация, обслуживание и вывод из эксплуатации. Оценка значимости и рисков: • Определение уровня конфиденциальности (общедоступная, внутренняя, конфиденциальная). • Анализ последствий от нарушения свойств ИБ (потеря доступности, целостности). Защита активов: • Организационные и технические меры, направленные на предотвращение утечек, повреждений или кражи информации

3	Методика COBIT: назначение, правила использования
	• Фундаментальные принципы: Удовлетворение потребностей стейкхолдеров, сквозной охват, интегрированная структура, целостный подход и разделение управления (governance) и менеджмента.
	• Домены ИТ-процессов: Процессы сгруппированы в четыре основных домена:
	  ○ Планирование и организация (PO): Стратегия, IT-структура.
	  ○ Проектирование и внедрение (AI): Разработка, приобретение, интеграция.
	  ○ Эксплуатация и сопровождение (DS): Техническая поддержка, инфраструктура.
	  ○ Мониторинг и оценка (ME): Контроль и аудит.
	• Цели контроля (Control Objectives): Подробное описание того, что необходимо контролировать в каждом процессе для снижения рисков.
	• Факторы влияния (Enablers): Принципы, процессы, организационные структуры, культура, информация, сервисы и люди, помогающие достичь целей.
	• Модель зрелости: Инструмент для оценки текущего состояния процессов (от 0 — несуществующий до 5 — оптимизированный).
	• Метрики и КПЭ: Ключевые индикаторы целей (KGI) и ключевые показатели результатов (KPI) для измерения эффективности ИТ.
	Структура отчета/документации по COBIT включает:
	1. Резюме для руководства.
	2. Описание текущей ИТ-ситуации.
	3. Выводы и рекомендации по улучшению

4	Система поддержки принятия парето-оптимальных решений в области проектирования системы защиты информации на предприятии 1. Введение и концепция системы • Актуальность: Проблема выбора оптимальной СЗИ в условиях ограниченного бюджета и многокритериальности (риск, стоимость, производительность) • Цель создания СППР: Определение множества Парето-оптимальных решений, обеспечивающих максимальный уровень защиты при минимальных затратах. • Определения: Множество Парето (Парето-эффективная граница) в задачах кибербезопасности. 2. Математическая модель задачи проектирования СЗИ

	• Входные параметры: Ресурсы предприятия, критичные информационные активы, перечень угроз и уязвимостей, каталог возможных мер защиты (технические, организационные)
	• Критерии оптимизации:
	  o Минимизация остаточного риска
	  o Минимизация стоимости внедрения и эксплуатации
	  o Минимизация негативного влияния на бизнес-процессы (время задержки, удобство)
	• Ограничения: Бюджетные лимиты, регуляторные требования (ФСТЭК/ФСБ), минимально допустимый уровень риска.
	• Целевая функция: Векторная оптимизация.
	3. Методы и алгоритмы поиска Парето-оптимальных решений
	• Подходы к решению:
	  o Скалярные методы (свертка критериев).
	  o Эволюционные алгоритмы (например, NSGA-II или MOEA/D) для нахождения фронта Парето в сложных системах.
	• Анализ Парето-эффективной границы: Визуализация вариантов, где улучшение одного критерия невозможно без ухудшения другого
	4. Архитектура СППР
	• Модуль сбора данных: Инвентаризация, оценка рисков.
	• База знаний: Перечень мер защиты, их стоимость и эффективность.
	• Оптимизационное ядро: Алгоритмы расчета.
	• Интерфейс пользователя (ЛПР): Визуализация результатов (паретовские графики), анализ "что-если".
	5. Практическая реализация и принятие решений
	• Методы выбора финального решения: Метод идеальной точки, метод экспертных оценок, анализ Парето-оптимального множества лицом, принимающим решения (ЛПР).
	• Пример работы системы: Проектирование защиты для типового предприятия с учетом ограниченного бюджета.
	6. Заключение
	• Преимущества использования СППР (обоснованность, экономическая эффективность)

5	Анализ и оценка рисков информационной безопасности с использованием нечеткой логики
	1. Введение в оценку рисков ИБ:
	  o Актуальность использования нечеткой логики при нехватке количественных данных.
	  o Ограничения классических вероятностных методов (оценка рисков как произведение вероятности на ущерб).
	  o Цели и задачи применения теории нечетких множеств.
	2. Методология нечеткого моделирования риска:
	  o Основные понятия: лингвистические переменные (угроза, уязвимость, ущерб, риск), терм-множества (низкий, средний, высокий).
	  o Построение функций принадлежности для входных факторов.
	  o Выбор алгоритма нечеткого вывода (обычно Мамдани — Mamdani).
	3. Разработка нечеткой системы оценки рисков (Fuzzy Expert System):
	  o Этап фаззификации: преобразование точных входных данных (например, баллы от 1 до 10) в нечеткие значения.

	○ База правил: формирование продукционных правил типа "ЕСЛИ-ТО" (например, ЕСЛИ «угроза высокая» И «уязвимость высокая», ТО «риск высокий»). ○ Дефаззификация: получение точного количественного значения уровня риска. 4. Применение инструментария (например, MATLAB Fuzzy Logic Toolbox): ○ Реализация разработанной модели в программной среде. ○ Визуализация поверхностей нечеткого вывода (зависимость риска от факторов). 5. Анализ результатов и верификация модели: ○ Пример расчета риска для конкретного сценария. ○ Сравнение результатов с традиционными методами. ○ Анализ чувствительности модели. Основные преимущества, описываемые в разделе: • Способность обрабатывать неполную или двусмысленную информацию. • Возможность использования естественного языка экспертов («высокий», «очень высокий»). • Повышение точности оценки за счет непрерывной шкалы рисков
6	Определение показателей защищенности информации при несанкционированном доступе Классификация и категорирование: Определение классов защищенности (К1, К2, К3) и уровней значимости информации на основе ее анализа. Оценка текущего состояния (ПЗИ): Расчет показателей защищенности, включая оценку уровня зрелости процессов защиты и соответствие нормативным требованиям. Анализ уязвимостей: Проверка инфраструктуры на наличие уязвимостей, вызванных ошибками конфигурации, ПО или программным обеспечением. Применяемые меры защиты: Включают технические средства (межсетевые экраны, антивирусы) и организационные процедуры. Сбор и анализ исходных данных: Процедура сбора информации о системе, необходимая для расчета показателей

4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Учебным планом не предусмотрено					
Всего					

4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 6.

Таблица 6 – Лабораторные занятия и их трудоемкость

№	Наименование лабораторных работ	Трудоемкость,	Из них	№

п/п		(час)	практической подготовки, (час)	раздела дисциплины
Семестр 7				
1	Лабораторная работа №1. Проектирование системы защиты информации с использованием модели с полным перекрытием множества угроз	3		1
2	Лабораторная работа №2. Классификация информационных активов предприятия	2		2
3	Лабораторная работа №3. Анализ рисков информационной безопасности с использованием методики COBIT	2		3
4	Система поддержки принятия парето-оптимальных решений в области проектирования системы защиты информации на предприятии	2		4
5	Лабораторная работа №5. Анализ и оценка рисков информационной безопасности с использованием нечеткой логики	4		5
6	Лабораторная работа №6. Определение показателей защищенности информации при несанкционированном доступе	4		6
	Всего	17		

4.5. Выполнение курсового проекта/ курсовой работы

Учебным планом не предусмотрено

4.6. Самостоятельная работа обучающихся

Виды самостоятельной работы и ее трудоемкость приведены в таблице 7.

Таблица 7 – Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 7, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	26	26
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	4	4
Домашнее задание (ДЗ)		
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)	8	8
Всего:	38	38

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.п. разделов 6-11.

6. Перечень печатных и электронных учебных изданий

Перечень печатных и электронных учебных изданий приведен в таблице 8.

Таблица 8– Перечень печатных и электронных учебных изданий

Шифр/ URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке (кроме электронных экземпляров)
004 М 54	Методология защиты информации : методические указания по выполнению лабораторных работ / С.-Петерб. гос. ун-т аэрокосм. приборостроения ; сост. Т. Н. Елина. - Санкт-Петербург : Изд-во ГУАП, 2022. - 50 с. : рис., табл. - Библиогр.: с. 49 (8 назв.). - Б. ц. - Текст : непосредственный.	5
004/М 87-604316-ED	Мошак Н. Н. Защищенные инфотелекоммуникации. Анализ и синтез [Электронный ресурс]: монография / Н. Н. Мошак; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Электрон. текстовые дан. - СПб.: Изд-во ГУАП, 2014. - 197 с.	50
004 М 87	Организация безопасного доступа к информационным ресурсам: учебное пособие / Н. Н. Мошак, Т. М. Татарникова. - СПб.: Изд-во ГУАП, 2014. - 121 с	40
Х404.3 М 48	Информационная безопасность и защита информации: учебное пособие/ В. П. Мельников, С. А. Клейменов, А. М. Петраков; ред. С. А Клейменов. - 5-е изд., стер. - М.: Академия, 2011. - 331 с.	25
004 Ш 22	Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие для СПО / В. Ф. Шаньгин. - М.: ФОРУМ: ИНФРА-М, 2016. - 416 с.	10
	Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. 392 с. http://znanium.com/catalog.php?bookinfo=474838	

7. Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

URL адрес	Наименование
	Не предусмотрено

8. Перечень информационных технологий

8.1. Перечень программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине.

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10– Перечень программного обеспечения

№ п/п	Наименование
	Не предусмотрено

8.2. Перечень информационно-справочных систем,используемых при осуществлении образовательного процесса по дисциплине

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11– Перечень информационно-справочных систем

№ п/п	Наименование
	Не предусмотрено

9. Материально-техническая база

Состав материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине, представлен в таблице12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Лекционная аудитория	
2	Мультимедийная лекционная аудитория	

10. Оценочные средства для проведения промежуточной аттестации

10.1. Состав оценочных средствдля проведения промежуточной аттестации обучающихся по дисциплине приведен в таблице 13.

Таблица 13 – Состав оценочных средств для проведения промежуточной аттестации

Вид промежуточной аттестации	Перечень оценочных средств
Зачет	Список вопросов; Тесты; Задачи.

10.2. В качестве критериев оценки уровня сформированности (освоения) компетенций обучающимися применяется 5-балльная шкала оценки сформированности компетенций, которая приведена в таблице 14. В течение семестра может использоваться 100-балльная шкала модульно-рейтинговой системы Университета, правила использования которой, установлены соответствующим локальным нормативным актом ГУАП.

Таблица 14 –Критерии оценки уровня сформированности компетенций

Оценка компетенции	Характеристика сформированных компетенций

5-балльная шкала	
«отлично» «зачтено»	Обучающийся: – глубоко и всесторонне усвоил программный материал; – уверенно, логично, последовательно и грамотно его излагает; – опираясь на знания основной и дополнительной литературы, тесно связывает усвоенные научные положения с практической деятельностью направления; – умело обосновывает и аргументирует выдвигаемые им идеи; – делает выводы и обобщения; – свободно владеет системой специализированных понятий. – правильно выполнил от 90% до 100% тестовых заданий**.
«хорошо» «зачтено»	Обучающийся: – твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; – не допускает существенных неточностей; – увязывает усвоенные знания с практической деятельностью направления; – аргументирует научные положения; – делает выводы и обобщения; – владеет системой специализированных понятий. – правильно выполнил от 70% до 89% тестовых заданий**.
«удовлетворительно» «зачтено»	– обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; – допускает несущественные ошибки и неточности; – испытывает затруднения в практическом применении знаний направления; – слабо аргументирует научные положения; – затрудняется в формулировании выводов и обобщений; – частично владеет системой специализированных понятий. – правильно выполнил от 51% до 69% тестовых заданий**.
«неудовлетворительно» «не зачтено»	– обучающийся не усвоил значительной части программного материала; – допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; – испытывает трудности в практическом применении знаний; – не может аргументировать научные положения; – не формулирует выводов и обобщений. – правильно выполнил менее 51% тестовых заданий**.

10.3. Типовые контрольные задания или иные материалы.

Вопросы (задачи) для экзамена представлены в таблице 15.

Таблица 15 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена	Код индикатора
	Учебным планом не предусмотрено	

Вопросы (задачи) для зачета / дифф. зачета представлены в таблице 16.

Таблица 16 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифф. зачета	Код индикатора
1	1. Теоретические основы анализа рисков ИБ • Определение «риска», «угрозы», «уязвимости» и «актива» в контексте ИБ. • Триада безопасности (CIA): конфиденциальность, целостность, доступность.	ПК-3.З.1

	• Цели и задачи анализа рисков (оценка ущерба, выбор мер защиты). • Принципы управления рисками ИБ: принятие, снижение, перенос, избежание.	
2	Методы и этапы оценки рисков • Основные этапы анализа рисков: идентификация, анализ, оценка. • Качественные методы оценки рисков (матрица вероятности и последствий). • Количественные методы оценки рисков (ALE — Annualized Loss Expectancy, SLE, ARO). • Комбинированные подходы к оценке рисков. • Определение источников рисков (антропогенные, техногенные, природные). • Идентификация активов и определение их ценности (классификация информации). • Анализ уязвимостей и оценка вероятности реализации угроз.	ПК-3.З.2
3	Теоретические основы и терминология • Основные понятия защиты информации: конфиденциальность, целостность, доступность (триада CIA), информационная безопасность, защита информации [1.1]. • Субъекты и объекты защиты информации. • Цели и задачи защиты информации в корпоративных и государственных системах. • Виды угроз безопасности информации (случайные/умышленные, внутренние/внешние). • Классификация нарушителей информационной безопасности.	ПК-3.У.1
4	Методологический подход к защите • Концепция эшелонированной (многоуровневой) защиты. • Принципы построения систем защиты информации (системность, непрерывность, законность, экономическая целесообразность). • Модель угроз: этапы разработки, структура, методы оценки вероятности реализации угроз. • Методы анализа рисков информационной безопасности (количественные и качественные методы). • Жизненный цикл системы защиты информации (планирование, проектирование, внедрение, эксплуатация, аудит).	ПК-3.У.2
5	Обработка и мониторинг рисков • Разработка планов обработки рисков (Risk Treatment Plan). • Выбор контрмер (технические, организационные, юридические). • Анализ остаточных рисков и принятие рисков руководством. • Мониторинг рисков и переоценка (пересмотр	ПК-3.В.1

	рисков при изменениях в инфраструктуре).	
6	Кейсы и практические аспекты • Примеры рисков ИБ: утечка данных, DDoS-атаки, потеря репутации. • Анализ рисков при внедрении новых IT-систем. • Взаимосвязь анализа рисков с непрерывностью бизнеса (BCP)	ПК-3.В.2
7	Нормативное обеспечение и стандарты • Обзор стандартов по управлению рисками: ISO/IEC 27005, NIST SP 800-30. • Связь риск-менеджмента с системой менеджмента ИБ (ISO/IEC 27001). • Российские нормативно-методические документы (ФСТЭК, Банк России).	ПК-6.З.1

Перечень тем для выполнения курсового проекта/ курсовой работы представлены в таблице 17.

Таблица 17 – Перечень тем для выполнения курсового проекта / курсовой работы

№ п/п	Примерный перечень тем для выполнения курсового проекта/ курсовой работы
	Учебным планом не предусмотрено

Вопросы для проведения промежуточной аттестации в виде тестирования представлены в таблице 18.

Таблица 18 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
	Правильный вариант ответа отмечен знаком + 1) К правовым методам, обеспечивающим информационную безопасность, относятся: - Разработка аппаратных средств обеспечения правовых данных - Разработка и установка во всех компьютерных правовых сетях журналов учета действий + Разработка и конкретизация правовых нормативных актов обеспечения безопасности 2) Основными источниками угроз информационной безопасности являются все указанное в списке: - Хищение жестких дисков, подключение к сети, инсайдерство + Перехват данных, хищение данных, изменение архитектуры системы - Хищение данных, подкуп системных администраторов, нарушение регламента работы 3) Виды информационной безопасности: + Персональная, корпоративная, государственная - Клиентская, серверная, сетевая - Локальная, глобальная, смешанная 4) Цели информационной безопасности – своевременное обнаружение, предупреждение: + несанкционированного доступа, воздействия в сети - инсайдерства в организации - чрезвычайных ситуаций	ПК-3.В.2

	5) Основные объекты информационной безопасности: + Компьютерные сети, базы данных - Информационные системы, психологическое состояние пользователей - Бизнес-ориентированные, коммерческие системы 6) Основными рисками информационной безопасности являются: - Искажение, уменьшение объема, перекодировка информации - Техническое вмешательство, выведение из строя оборудования сети + Потеря, искажение, утечка информации 7) К основным принципам обеспечения информационной безопасности относится: + Экономической эффективности системы безопасности - Многоплатформенной реализации системы - Усиления защищенности всех звеньев системы 8) Основными субъектами информационной безопасности являются: - руководители, менеджеры, администраторы компаний + органы права, государства, бизнеса - сетевые базы данных, фаерволлы 9) К основным функциям системы безопасности можно отнести все перечисленное: + Установление регламента, аудит системы, выявление рисков - Установка новых офисных приложений, смена хостинг-компании - Внедрение аутентификации, проверки контактных данных пользователей тест 10) Принципом информационной безопасности является принцип недопущения: + Неоправданных ограничений при работе в сети (системе) - Рисков безопасности сети, системы - Презумпции секретности 11) Принципом политики информационной безопасности является принцип: + Невозможности миновать защитные средства сети (системы) - Усиления основного звена сети, системы - Полного блокирования доступа при риск-ситуациях 12) Принципом политики информационной безопасности является принцип: + Усиления защищенности самого незащищенного звена сети (системы) - Перехода в безопасное состояние работы сети, системы - Полного доступа пользователей ко всем ресурсам сети, системы 13) Принципом политики информационной безопасности является принцип: + Разделения доступа (обязанностей, привилегий) клиентам сети (системы) - Одноуровневой защиты сети, системы - Совместимых, однотипных программно-технических средств сети, системы 14) К основным типам средств воздействия на компьютерную сеть относится: - Компьютерный сбой	

	+ Логические закладки («мины») - Аварийное отключение питания 15) Когда получен спам по e-mail с приложенным файлом, следует: - Прочитать приложение, если оно не содержит ничего ценного – удалить - Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама + Удалить письмо с приложением, не раскрывая (не читая) его 16) Принцип Кирхгофа: - Секретность ключа определена секретностью открытого сообщения - Секретность информации определена скоростью передачи данных + Секретность закрытого сообщения определяется секретностью ключа 17) ЭЦП – это: - Электронно-цифровой преобразователь + Электронно-цифровая подпись - Электронно-цифровой процессор 18) Наиболее распространены угрозы информационной безопасности корпоративной системы: - Покупка нелицензионного ПО + Ошибки эксплуатации и неумышленного изменения режима работы системы - Сознательного внедрения сетевых вирусов 19) Наиболее распространены угрозы информационной безопасности сети: - Распределенный доступ клиент, отказ оборудования - Моральный износ сети, инсайдерство + Сбой (отказ) оборудования, нелегальное копирование данных тест_20) Наиболее распространены средства воздействия на сеть офиса: - Слабый трафик, информационный обман, вирусы в интернет + Вирусы в сети, логические мины (закладки), информационный перехват - Компьютерные сбои, изменение администрирования, топологии 21) Утечкой информации в системе называется ситуация, характеризуемая: + Потерей данных в системе - Изменением формы информации - Изменением содержания информации 22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются: + Целостность - Доступность - Актуальностьl 23) Угроза информационной системе (компьютерной сети) – это: + Вероятное событие - Детерминированное (всегда определенное) событие - Событие, происходящее периодически 24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется: - Регламентированной	

	- Правовой + Защищаемой 25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке: + Программные, технические, организационные, технологические - Серверные, клиентские, спутниковые, наземные - Личные, корпоративные, социальные, национальные 26) Окончательно, ответственность за защищенность данных в компьютерной сети несет: + Владелец сети - Администратор сети - Пользователь сети 27) Политика безопасности в системе (сети) – это комплекс: + Руководств, требований обеспечения необходимого уровня безопасности - Инструкций, алгоритмов поведения пользователя в сети - Нормы информационного права, соблюдаемые в сети 28) Наиболее важным при реализации защитных мер политики безопасности является: - Аудит, анализ затрат на проведение защитных мер - Аудит, анализ безопасности + Аудит, анализ уязвимостей, риск-ситуаций	

Перечень тем контрольных работ по дисциплине обучающихся заочной формы обучения, представлены в таблице 19.

Таблица 19 – Перечень контрольных работ

№ п/п	Перечень контрольных работ
	Не предусмотрено

10.4. Методические материалы, определяющие процедуры оценивания индикаторов, характеризующих этапы формирования компетенций, содержатся в локальных нормативных актах ГУАП, регламентирующих порядок и процедуру проведения текущего контроля успеваемости и промежуточной аттестации обучающихся ГУАП.

11. Методические указания для обучающихся по освоению дисциплины

11.1. Методические указания для обучающихся по освоению лекционного материала .

Основное назначение лекционного материала – логически стройное, системное, глубокое и ясное изложение учебного материала. Назначение современной лекции в рамках дисциплины не в том, чтобы получить всю информацию по теме, а в освоении фундаментальных проблем дисциплины, методов научного познания, новейших достижений научной мысли. В учебном процессе лекция выполняет методологическую, организационную и информационную функции. Лекция раскрывает понятийный аппарат конкретной области знания, её проблемы, дает цельное представление о дисциплине, показывает взаимосвязь с другими дисциплинами.

Планируемые результаты при освоении обучающимися лекционного материала:

– получение современных, целостных, взаимосвязанных знаний, уровень которых определяется целевой установкой к каждой конкретной теме;

– получение опыта творческой работы совместно с преподавателем;

– развитие профессионально-деловых качеств, любви к предмету и самостоятельного творческого мышления.

– появление необходимого интереса, необходимого для самостоятельной работы;

– получение знаний о современном уровне развития науки и техники и о прогнозе их развития на ближайшие годы;

– научиться методически обрабатывать материал (выделять главные мысли и положения, приходить к конкретным выводам, повторять их в различных формулировках);

– получение точного понимания всех необходимых терминов и понятий.

Лекционный материал может сопровождаться демонстрацией слайдов и использованием раздаточного материала при проведении коротких дискуссий об особенностях применения отдельных тематик по дисциплине.

Структура предоставления лекционного материала:

– Методы анализа рисков информационной безопасности

– Информационные активы предприятия

– Методика COBIT: назначение, правила использования

– Система поддержки принятия парето-оптимальных решений в области проектирования системы защиты информации на предприятии

– Анализ и оценка рисков информационной безопасности с использованием нечеткой логики

– Определение показателей защищенности информации при несанкционированном доступе

11.2. Методические указания для обучающихся по выполнению лабораторных работ

В ходе выполнения лабораторных работ обучающийся должен углубить и закрепить знания, практические навыки, овладеть современной методикой и техникой эксперимента в соответствии с квалификационной характеристикой обучающегося. Выполнение лабораторных работ состоит из экспериментально-практической, расчетно-аналитической частей и контрольных мероприятий.

Выполнение лабораторных работ обучающимся является неотъемлемой частью изучения дисциплины, определяемой учебным планом, и относится к средствам, обеспечивающим решение следующих основных задач обучающегося:

– приобретение навыков исследования процессов, явлений и объектов, изучаемых в рамках данной дисциплины;

– закрепление, развитие и детализация теоретических знаний, полученных на лекциях;

– получение новой информации по изучаемой дисциплине;

– приобретение навыков самостоятельной работы с лабораторным оборудованием и приборами.

Задание и требования к проведению лабораторных работ

Решение проблемы защиты информации на предприятии связано с гарантированным обеспечением трех ее главных составляющих: доступности, целостности и конфиденциальности информации. Задача обеспечения информационной безопасности (ИБ) состоит в разработке модели представления системы и процессов ИБ, которая на основе научно-методического аппарата позволяла бы решать задачи создания, использования и оценки эффективности системы защиты информации для проектируемых и существующих информационных систем.

В лабораторных работах рассматриваются задачи и программный инструментарий для их решения. В частности: проектирование систем защиты информации с

использованием модели с полным перекрытием множества угроз; анализ и управление рисками информационной безопасности с использованием различных методик; система поддержки принятия парето-оптимальных решений в области проектирования системы защиты информации; определение показателей защищенности информации при несанкционированном доступе; методики анализа рисков информационной безопасности для малого и среднего бизнеса; анализ рисков информационной безопасности с использованием нечеткой логики.

Структура и форма отчета о лабораторной работе

Отчет по лабораторной работе представляет собой небольшой научно-практический отчет, являющийся итогом проведенной студентом работы, представленный для дальнейшей защиты. Отчеты по лабораторным работам должны содержать исчерпывающее описание проделанной студентом работы, позволять оценить полученные результаты, а также степень выполнения индивидуального задания. В отчете по лабораторной работе должны содержаться следующие элементы:

- титульный лист;
- цель работы;
- краткие теоретические сведения;
- описание математической модели;
- описание и результаты проводимых расчетов
- анализ результатов работы модели;
- выводы.

Цель работы должна отражать тему лабораторной работы, а также индивидуальные задачи, поставленные студенту для реализации в рамках лабораторной работы. По объему цель работы в зависимости от сложности и многозадачности работы составляет от нескольких строк до 0,5 страницы.

В кратких теоретических сведениях излагается общее описание изучаемого в работе явления или процесса, приводятся необходимые расчетные формулы. Материал раздела не должен копировать содержание методического пособия или учебника по данной теме, а ограничивается изложением основных понятий и законов, расчетных формул, таблиц, требующихся для дальнейшей обработки полученных результатов. Объем этого раздела не должен превышать трети всего отчета.

Описание математической модели может быть выполнено в формульном виде, представлено графически, таблично или блок-схемами, в зависимости от используемой модели.

Раздел отчета «Анализ результатов работы» должен содержать подробный анализ полученных результатов. Следует сравнить полученные результаты с известными литературными данными, обсудить их соответствие существующим теоретическим моделям. Если обнаружено несоответствие полученных результатов и теоретических расчетов или литературных данных, необходимо обсудить возможные причины этих несоответствий.

В выводах по лабораторной работе кратко излагаются результаты, которые удалось или не удалось достичь в ходе выполненной работы.

Отчет по лабораторной работе оформляется на писчей бумаге стандартного формата А4 на одной стороне листа, которые сшиваются в скоросшивателе или переплетаются. Допускается оформление отчета по лабораторной работе только в электронном виде.

Требования к оформлению отчета о лабораторной работе

Теоретическая часть должна содержать минимум необходимых теоретических сведений о предметной области. Не следует копировать целиком или частично методическое пособие (описание) лабораторной работы или разделы учебника.

В разделе Программное обеспечение необходимо описать, с помощью каких инструментальных средств и каким образом были разработаны модели и получены результаты. Рисунки, блок-схемы, описание модели и её особенностей, необходимость отладки – все это должно быть представлено в указанном разделе.

Раздел Результаты включает в себя скриншоты программного приложения, полученные при выполнении лабораторной работы. Рисунки, графики и таблицы нумеруются и подписываются заголовками.

Выводы не должны быть простым перечислением того, что сделано. Здесь важно отметить, какие новые знания о предмете исследования были получены при выполнении работы, к чему привело обсуждение результатов, насколько выполнена заявленная цель работы. Выводы по работе каждый студент делает самостоятельно. В случае необходимости в конце отчёта приводится Список литературы, использованной при подготовке к работе. В тексте отчёта делаются краткие ссылки на литературу (учебники, справочники, иные источники…) номером в квадратных скобках, напр., [1]. Литературные источники нумеруются по мере их появления в тексте отчёта. В конце отчёта даётся их подробный список. На все источники списка литературы должны быть ссылки в тексте отчёта, там, где это необходимо.

При сдаче отчёта преподаватель может сделать устные и письменные замечания, задать дополнительные вопросы. Все ответы на дополнительные вопросы, обсуждения выполняются студентом на отдельных листах, включаемых в отчёт (при этом в тексте основного отчёта делается сноска или другой значок, которому будет соответствовать новый материал). При этом письменные замечания преподавателя должны остаться в тексте для ясности динамики работы над отчётом.

Объём отчёта должен быть оптимальным для понимания того, что и как сделал студент, выполняя работу. Обязательные требования к отчёту включают общую и специальную грамотность изложения, а также аккуратность оформления.

После приёма преподавателем отчёт хранится на кафедре.

Методические указания по прохождению лабораторных работ имеются в изданном виде, и приведены в таблице 8.

11.3. Методические указания для обучающихся по прохождению самостоятельной работы

В ходе выполнения самостоятельной работы, обучающийся выполняет работу по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

В процессе выполнения самостоятельной работы у обучающегося формируется целесообразное планирование рабочего времени, которое позволяет ему развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивает высокий уровень успеваемости в период обучения, помогает получить навыки повышения профессионального уровня.

Методическими материалами, направляющими самостоятельную работу обучающихсяявляются:

- учебно-методический материал по дисциплине;
- методические указания по выполнению контрольных работ (для обучающихся по заочной форме обучения).

11.4. Методические указания для обучающихся по прохождению текущего контроля успеваемости.

Текущий контроль успеваемости предусматривает контроль качества знаний обучающихся, осуществляемого в течение семестра с целью оценивания хода освоения дисциплины.

Для успешного прохождения текущего контроля необходимо выполнить лабораторные работы, загрузить их в личный кабинет и пройти процедуру защиты каждой работы. Оценки за работы выставляются по пятибалльной шкале.

11.5. Методические указания для обучающихся по прохождению промежуточной аттестации.

Промежуточная аттестация обучающихся предусматривает оценивание промежуточных и окончательных результатов обучения по дисциплине. Она включает в себя:

– зачет – это форма оценки знаний, полученных обучающимся в ходе изучения учебной дисциплины в целом или промежуточная (по окончании семестра) оценка знаний обучающимся по отдельным разделам дисциплины с аттестационной оценкой «зачтено» или «не зачтено».

Для успешного прохождения промежуточной аттестации необходимо за защищенные лабораторные работы получить интегральную оценку не ниже «удовлетворительно».

Лист внесения изменений в рабочую программу дисциплины

Дата внесения изменений и дополнений. Подпись внесшего изменения	Содержание изменений и дополнений	Дата и № протокола заседания кафедры	Подпись зав. кафедрой