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
«Комплексная защита объектов информатизации»
(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)

проф.,д.т.н.,проф. (должность, уч. степень, звание) 20.02.26 (подпись, дата) С.Г. Фомичева (инициалы, фамилия)

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

Заведующий кафедрой № 33

д.т.н.,проф. (уч. степень, звание) 20.02.26 (подпись, дата) С.В. Беззатеев (инициалы, фамилия)

Заместитель директора института №3 по методической работе

доц.,к.т.н. (должность, уч. степень, звание) 20.02.26 (подпись, дата) Н.В. Решетникова (инициалы, фамилия)

Аннотация

Дисциплина «Комплексная защита объектов информатизации» 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:

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-6 «Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю»

ОПК-10 «Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты»

ОПК-12 «Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений»

ОПК-1.4 «Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями»

Дисциплина «Комплексная защита объектов информатизации» изучает принципы создания Комплексных систем защиты информации (КСЗИ). Ее главная цель — обеспечение конфиденциальности, целостности и доступности данных за счет объединения организационных, правовых, физических и технических мер.

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

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме зачета (8 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 дисциплины «Комплексная защита объектов информатизации» заключается в формировании у студентов теоретических знаний и практических навыков для создания, внедрения и эксплуатации систем, обеспечивающих безопасность, конфиденциальность, целостность и доступность информации

1.2. Дисциплина входит в состав обязательной части 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
Общепрофессиональные компетенции	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.В.1 владеет навыками оценки и анализа необходимости внедрения средств информационной безопасности в процессы производства
Общепрофессиональные компетенции	ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации,	ОПК-6.З.2 знает задачи органов защиты государственной тайны и служб защиты информации на предприятиях ОПК-6.У.1 умеет разрабатывать модели угроз и модели нарушителя объекта информатизации

	Федеральной службы по техническому и экспортному контролю	
Общепрофессиональные компетенции	ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ОПК-10.З.3 знает принципы формирования политики информационной безопасности организации ОПК-10.В.1 владеет навыками комплексного всестороннего анализа информационной безопасности объектов защиты и их отдельных элементов
Общепрофессиональные компетенции	ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ОПК-12.З.3 знает требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации ОПК-12.У.2 умеет анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации ОПК-12.У.4 умеет оценивать информационные риски в автоматизированных системах ОПК-12.В.1 владеет навыками оценки эффективности применяемых средств защиты информации, определение их уровня защищенности
Общепрофессиональные компетенции по направленности	ОПК-1.4 Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	ОПК-1.4.В.1 владеет навыками оценки целесообразности разработки и внедрения отдельных компонентов систем защиты информации

2. Место дисциплины в структуре ОП

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

- Основы информационной безопасности;
- Документоведение и конфиденциальное делопроизводство;
- Инженерно-технические средства защиты информации

Знания, полученные при изучении материала данной дисциплины, имеют самостоятельное значение.

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
		№8
1	2	3
Общая трудоемкость дисциплины, ЗЕ/ (час)	2/ 72	2/ 72
Из них часов практической подготовки		
Аудиторные занятия, всего час.	30	30
в том числе:		
лекции (Л), (час)	10	10
практические/семинарские занятия (ПЗ), (час)		
лабораторные работы (ЛР), (час)	20	20
курсовой проект (работа) (КП, КР), (час)		
экзамен, (час)		
Самостоятельная работа, всего (час)	42	42
***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 8					
Раздел 1 – Проблема обеспечения информационной безопасности (ИБ) предприятия	2		8		11
Раздел 2 – Основные виды угроз ИБ предприятия	3		4		10
Раздел 3 – Средства защиты информационныхресурсов предприятия	3		4		10
Раздел 4 – Политика обеспечения информационной безопасности предприятия.	2		4		11
Итого в семестре:	10		20		42
Итого	10	0	20	0	42

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	Раздел 1 – Проблема обеспечения информационной безопасности (ИБ) предприятия. Тема 1.1 – Основные положения информационной безопасности. Определение и цели информационной безопасности. Механизмы и инструментарии информационной безопасности. Основные направления ИБ. Тема 1.2 – Задачи и принципы организации службы информационной безопасности. Задачи службы информационной безопасности. Взаимодействие службы ИБ с администраторами сетей и систем. Принятие решений по вопросам ИБ. Состав службы ИБ и подбор кадров. Тема 1.3 – Классификация объектов и субъектов ИБ. Классификация информационных объектов. Классификатор средств обработки информации. Классификатор субъектов информационного пространства. Роли и ответственность субъектов. Принципы распределения прав и ответственности. Сопоставление ролей функциональным обязанностям и классам обрабатываемой информации.
2	Раздел 2 – Основные виды угроз информационной безопасности предприятия. Тема 2.1 – Модель нападения. Классификация атак. Модели реализации атак на информационные системы предприятия. Социальная инженерия. Закладки в аппаратном обеспечении. Разграничение доступа. Атаки на средства аутентификации. Биометрические средства аутентификации. Токены. Пароли. Удаленные атаки. Маскировка. Атаки на маршрутизацию. Атаки на серверы и клиентов. Атаки на поток данных. Тема 2.2 – Управление рисками. Методика управления рисками. Методики оценки рисков.
3	Раздел 3 – Средства защиты информационных ресурсов предприятия. Тема 3.1 – Контроль физического доступа. Система охраны периметра. Система контроля и управления доступом. Система видеонабдюдения. Система охранной сигнализации. Система хранения. Тема 3.2 – Протоколы сетевой безопасности. Протоколы аутентификации: PAP, CHAP, RADIUS,

	TACACS, Kerberos, S/Key. Протоколы прикладного уровня: SHTTP. Протоколы транспортного уровня: SSL, Secure Shell, SOCKS. Протоколысетевого уровня: IPSec, L2F, PPTP, L2TP. Тема 3.3. Автоматизированные средства безопасности. Антивирусы. Межсетевые экраны. Технология VPN.Криптографические средства. Сканеры уязвимостей. Системы обнаружения атак.
4	Раздел 4 – Политика обеспечения информационной безопасности предприятия.

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

№п/п	Наименование лабораторных работ	Трудоемкость,(час)	Из них практической подготовки, (час)	№ раздела дисциплины
Семестр 8				
1	Подбор кадров службы ИБ предприятия	4		1
2	Распределения прав и ответственности	4		1
3	Протокол Kerberos	4		2
4	Антивирусная защита.	4		3
5	Методология разработки политики предприятия	4		4
Всего		20		

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 8, час

1	2	3
Изучение теоретического материала дисциплины (ТО)	20	20
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	12	12
Домашнее задание (ДЗ)		
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)	10	10
Всего:	42	42

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)
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.	23
004.49(075) Ш 22	Защита компьютерной информации/В.Ф. Шаньгин. - ДМКПресс, 2010. 544 с.	2
004.7 Б 43	Администрирование в информационных системах: учебноепособие/ М. Н. Беленькая, С. Т. Малиновский, Н. В. Яковенко. - М.: Горячая линия - Телеком, 2011. - 399 с.	10
http://www.znanium.com/bookread.php?book=175658	Комплексная система защиты информации на предприятии: учебное пособие/Н.В. Гришина. - М.: Форум, 2009, 240 с.	

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
Lms.guap.ru	Система дистанционного обучения ГУАП (СДО ГУАП)
rsv.ru	Платформа “Россия – страна возможностей”
leader-id.ru	Платформа “Leader-ID”

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 5-балльная шкала	Характеристика сформированных компетенций
«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	Концепция комплексной защиты информации Обобщенная модель системы безопасности Постановка задачи обеспечения комплексной защиты информации в системе	ОПК-1.В.1
2	Выделение существенных угроз . Отсеивающие эксперименты.	ОПК-6.З.2
3	Выбор параметров элементов модели Модели связей	ОПК-6.У.1
4	Выявление основных информационных угроз Оценка влияния угроз на основе моделирования системы	ОПК-10.З.3
5	Этапы построения модели системы Типовые элементы модели	ОПК-10.В.1
6	Сети Петри, как аппарат описания системы Модель функционирования системы Имитационная модель системы	ОПК-12.З.3
7	Методы упрощения модели Метод существенной выборки Метод расслоенной выборки Метод дополнительной переменной	ОПК-12.У.2
8	Эксперименты с моделью системы Экспертные оценки параметров системы	ОПК-12.У.4
9	Выделение существенных угроз. Дисперсионный анализ Кибернетическая модель системы	ОПК-12.В.1
10	Задача оптимизации системы защиты в условиях ограниченныхресурсов Методы оптимизации системы защиты Методология создания системы комплексной защиты	ОПК-1.4.В.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
	Как называется технический канал утечки, возникающий из-за наводок информационных сигналов в цепи электропитания и заземления оборудования? • Акустоэлектрический канал • Оптико-электронный канал	ОПК-1.В.1

	• [✓] Канал побочных электромагнитных излучений и наводок (ПЭМИН) • Радиоэлектронный канал	
	Какое техническое средство относится к элементам физической защиты первого рубежа (периметра) объекта информатизации? • Аппаратный межсетевой экран • Биометрический считыватель на двери серверной • [✓] Противотаранное устройство и охранное ограждение с извещателями • Программный комплекс обнаружения вторжений (IDS)	ОПК-6.З.2
	Какой руководящий документ ФСТЭК России определяет требования к средствам вычислительной техники по уровням контроля отсутствия недекларированных возможностей (НДВ)? • Приказ ФСТЭК № 21 • [✓] Требования по уровням доверия (взамен старых руководящих документов по НДВ) • Приказ ФСТЭК № 17 • Специальные требования и рекомендации (СТР)	ОПК-6.У.1
	Каков максимальный срок действия «Аттестата соответствия» на объект информатизации, предназначенный для обработки конфиденциальной информации (при условии неизменности условий эксплуатации)? • 1 год • 3 года • [✓] 5 лет • Аттестат выдается бессрочно	ОПК-10.З.3
	Какая мера является наиболее эффективной для защиты конфиденциальных разговоров в помещении от съема информации через оконные стекла с помощью лазерных систем? • Установка плотных тканевых штор • Использование стеклопакетов с аргоновым наполнением • [✓] Установка виброакустических датчиков-шумоизлучателей (пьезоэлементов) на стекла • Покрытие стекол зеркальной тонировочной пленкой	ОПК-10.В.1
	На основе какого главного критерия устанавливается категория важности объекта информатизации (или класс защищенности автоматизированной системы)? • Стоимость закупленного серверного оборудования • [✓] Уровень конфиденциальности (ценности) информации и масштаб ущерба от ее нарушения • Количество сотрудников, имеющих доступ в здание • Общая площадь помещений, занимаемых объектом	ОПК-12.З.3
	Какой класс средств криптографической защиты информации (СКЗИ) является минимально необходимым для защиты информации, содержащей государственную тайну уровня «особой важности»? • Класс КС1 • Класс КВ • Класс КА	ОПК-12.У.2

	• [✓] Класс КВ2 / КА (высшие классы СКЗИ, сертифицированные ФСБ)	
	Как называется процедура проверки соответствия существующей системы защиты объекта требованиям законодательства, стандартов и внутренних регламентов? • Моделирование угроз • [✓] Аудит информационной безопасности • Проектирование системы защиты • Лицензирование деятельности	ОПК-12.У.4
	Какое устройство обязательно устанавливается на линиях электропитания и слаботочных линиях, выходящих за пределы контролируемой зоны выделенного помещения? • Автоматический выключатель (автомат) • [✓] Помехоподавляющий сетевой фильтр • Источник бесперебойного питания (ИБП) • Распределительная коробка	ОПК-12.В.1
	Что из перечисленного НЕ входит в структуру комплексной системы защиты объекта информатизации? • Правовая подсистема • Инженерно-техническая подсистема • Организационная подсистема • [✓] Маркетинговая подсистема продвижения услуг	ОПК-1.4.В.1

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 *(если предусмотрено учебным планом по данной дисциплине).*

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:

Раздел 1 – Проблема обеспечения информационной безопасности (ИБ)предприятия.
Тема 1.1 – Основные положения информационной безопасности.
Тема 1.2 – Задачи и принципы организации службы информационнойбезопасности.
Тема 1.3 – Классификация объектов и субъектов ИБ.
Раздел 2 – Основные виды угроз информационной безопасности предприятия.
Тема 2.1 – Модель нападения.
Тема 2.2 – Управление рисками.
Раздел 3 – Средства защиты информационных ресурсов предприятия.
Тема 3.1 – Контроль физического доступа.
Тема 3.2 – Протоколы сетевой безопасности.
Тема 3.3. Автоматизированные средства безопасности.
Раздел 4 - Политика обеспечения информационной безопасности предприятия.

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

Вариант задания по каждой лабораторной работе обучающийся получает в соответствии с номером в списке группы. Перед проведением лабораторной работы обучающемуся следует внимательно ознакомиться с методическими указаниями по ее выполнению. В соответствии с заданием обучающийся должен подготовить

необходимые данные, получить от преподавателя допуск к выполнению лабораторной работы, выполнить указанную последовательность действий, получить требуемые результаты, оформить и защитить отчет по лабораторной работе.

Структура и форма отчета о лабораторной работе

Отчет о лабораторной работе должен включать в себя: титульный лист, формулировку задания, теоретические положения, используемые при выполнении лабораторной работы, описание процесса выполнения лабораторной работы, полученные результаты и выводы.

Требования к оформлению отчета о лабораторной работе

По каждой лабораторной работе выполняется отдельный отчет. Титульный лист оформляется в соответствии с шаблоном (образцом) приведенным на сайте ГУАП (www.guap.ru) в разделе «Сектор нормативной документации». Текстовые и графические материалы оформляются в соответствии с действующими ГОСТами и требованиями, приведенными на сайте ГУАП (www.guap.ru) в разделе «Сектор нормативной документации».

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.

Текущий контроль успеваемости проводится в течение семестра. Его главная цель — проверить, как студент усваивает лекционный материал, справляется с практическими заданиями и лабораторными работами.

Результаты контроля влияют на:

- Допуск к промежуточной аттестации (экзамену или зачету).
- Формирование рейтингового балла (при наличии балльно-рейтинговой системы — БРС).
- Возможность получения оценки «автоматом».

Формы текущего контроля и порядок их прохождения

Компьютерное или письменное тестирование

Оценивает теоретические знания стандартов (ГОСТы серии 50922, ИСО/МЭК 27001), законов (ФЗ-149, ФЗ-152) и принципов выявления каналов утечки информации (ПЭМИН, акустические).

Как проходить: Изучите конспекты лекций и нормативно-правовую базу. Внимательно читайте формулировку вопроса (иногда требуется выбрать несколько вариантов ответа).

Сроки: Проводится на практических занятиях или в электронной среде вуза (например, Moodle) строго в установленные преподавателем дедлайны.

Выполнение и защита лабораторных работ

Практическая часть включает в себя моделирование угроз, расчет зон эвакуации, выбор средств защиты (генераторов шума, сетевых фильтров) и проектирование контролируемой зоны.

Как проходить: Оформляйте отчеты строго по ГОСТу или методичке кафедры. Обязательно проверяйте наличие выводов к каждой работе.

На защите: Студент должен устно объяснить ход выполнения работы, выбор конкретных технических средств защиты и ответить на контрольные вопросы.

Решение ситуационных задач (кейсов)

Вам дается описание условного объекта (например, коммерческий банк или государственное учреждение). Задача — провести аудит, выявить уязвимые места и предложить комплексную систему защиты.

Как проходить: Обосновывайте каждое решение ссылкой на нормативные акты (приказы ФСТЭК №17/21, требования ФСБ) и принципы экономической целесообразности.

Критерии оценивания

Применяется стандартная четырехбалльная система или шкала БРС:

«Отлично» (86–100 баллов): Студент демонстрирует глубокие знания нормативной базы и инженерно-технических мер защиты, свободно владеет терминологией, без ошибок решает практические задачи, выполняет работы в срок.

«Хорошо» (71–85 баллов): Материал усвоен в полном объеме. Студент ориентируется в технологиях и законах, но при ответе допускает незначительные погрешности или незначительно нарушает сроки сдачи отчетов.

«Удовлетворительно» (51–70 баллов): Знания носят фрагментарный характер. Студент понимает основы комплексной защиты, но путается в классах СКЗИ, требованиях регуляторов (ФСТЭК/ФСБ) или с трудом решает практические задачи.

«Неудовлетворительно» (менее 50 баллов): Ключевые понятия дисциплины не освоены, лабораторные работы не выполнены или не защищены, тесты провалены.

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».

Зачет проводится в конце семестра в соответствии с утвержденным расписанием занятий.

Условие допуска: Для получения допуска к зачету студент обязан успешно выполнить и защитить все предусмотренные учебным планом лабораторные работы, а также пройти текущие контроли (тесты).

«Зачет автоматический»: Студенты, набравшие высокий рейтинговый балл в течение семестра, могут освобождаться от устной/письменной процедуры зачета с выставлением оценки «зачтено».

Формы проведения зачета

Устный опрос по билетам: Билет включает два теоретических вопроса (например, нормативно-правовое регулирование и каналы утечки информации) и одну практическую задачу. На подготовку отводится не менее 30–40 минут.

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