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

Кафедра №34

«УТВЕРЖДАЮ»
Руководитель направления
проф.,д.т.н.,доц.
(должность, уч. степень, звание)
С.В. Беззатеев
(подпись)
«24» июня 2021 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Методология защиты информации»
(Название дисциплины)

Код направления	10.05.05
Наименование направления/ специальности	Безопасность информационных технологий в правоохранительной сфере
Наименование направленности	Технологии защиты информации в правоохранительной сфере
Форма обучения	очная

Санкт-Петербург– 2019 г.

Лист согласования рабочей программы дисциплины

Программу составил(а)
доц.,к.э.н.,доц. 24.06.21 Т.Н. Елина
должность, уч. степень, звание — подпись, дата — инициалы, фамилия

Программа одобрена на заседании кафедры № 34
«24» июня 2021 г., протокол № 11

Заведующий кафедрой № 34
проф.,д.т.н.,доц. «24» июня 2021 г. С.В. Беззатеев
должность, уч. степень, звание — подпись, дата — инициалы, фамилия

Ответственный за ОП 10.05.05(01)
доц.,к.т.н.,доц. 24.06.21 В.А. Мыльников
должность, уч. степень, звание — подпись, дата — инициалы, фамилия

Заместитель директора института (декана факультета) № 3 по методической работе
доц.,к.э.н.,доц. 24.06.21 Г.С. Армашова-Тельник
должность, уч. степень, звание — подпись, дата — инициалы, фамилия

Аннотация

Дисциплина «Методология защиты информации» входит в базовую часть образовательной программы подготовки обучающихся по специальности «10.05.05 «Безопасность информационных технологий в правоохранительной сфере» специализации «Технологии защиты информации в правоохранительной сфере». Дисциплина реализуется кафедрой №34.

Дисциплина нацелена на формирование у выпускника

профессиональных компетенций:

ПК-1 «способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз»,

ПК-2 «способность применять технические и программно-аппаратные средства обработки и защиты информации»,

ПК-17 «способность организовывать подготовку и представлять объект информатизации в ходе аттестации на соответствие требованиям государственных и ведомственных нормативных документов»,

ПК-18 «способность разрабатывать предложения по совершенствованию системы управления безопасностью информации»,

ПК-19 «способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности».

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, практические занятия, самостоятельная работа студента.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме диффренцированного зачета.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов.

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. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения дисциплины студент должен обладать следующими компетенциями:

ПК-1 «способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз»:

знать – существующие меры по обеспечению безопасности информации;

уметь – формировать и реализовывать комплекс мер по обеспечению безопасности информации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз

владеть навыками – реализации комплекса мер по обеспечению безопасности информации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз

иметь опыт деятельности - в реализации комплекса мер по обеспечению безопасности на конкретном объекте защиты

ПК-2 «способность применять технические и программно-аппаратные средства обработки и защиты информации»:

знать – современные базу программно-аппаратных и криптографических средств защиты информации;

уметь – выбирать и применять программно-аппаратные и криптографические средства защиты информации в зависимости от условий задачи защиты информации;

владеть навыками – решения задач выбора программно-аппаратных и криптографических средств защиты информации при известных условиях их применения;

иметь опыт деятельности – в применении программно-аппаратных и криптографических средств защиты информации в зависимости от условий задачи защиты информации;

ПК-17 «способность организовывать подготовку и представлять объект информатизации в ходе аттестации на соответствие требованиям государственных и ведомственных нормативных документов»:

знать – существующую нормативную базу для проведения аттестации объекта информатизации;

уметь – организовывать подготовку и представлять объект информатизации в ходе аттестации на предмет соответствия требованиям государственных и ведомственных нормативных документов

владеть навыками – подготовки объекта информатизации для аттестации на предмет соответствия требованиям государственных и ведомственных нормативных документов;

иметь опыт деятельности – в организации подготовки и представлении объекта информатизации для аттестации;

ПК-18 «способность разрабатывать предложения по совершенствованию системы управления безопасностью информации»:

знать – назначение и структуру системы управления безопасностью информации;

уметь – предложить способы совершенствования системы управления безопасностью информации;

владеть навыками – методического подхода к совершенствования системы управления безопасностью информации;

иметь опыт деятельности – в разработке предложений по совершенствованию системы управления безопасностью информации;

ПК-19 «способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности»:

знать – отечественные и зарубежные стандарты в области информационной безопасности;

уметь – проводить анализ состояния безопасности информации на объектах и в отдельных системах с использованием отечественных и зарубежных стандартов

владеть навыками – методическим обеспечением анализа состояния безопасности информации на объектах и системах;

иметь опыт деятельности – в применении методического обеспечения анализа состояния безопасности информации на конкретных объектах и в системах с использованием отечественных и зарубежных стандартов.

2. Место дисциплины в структуре ОП

Дисциплина базируется на знаниях, ранее приобретенных студентами при изучении следующих дисциплин:

- Криптографическая защита информации
- Программно-аппаратная защита информации
- Теория информационной безопасности.

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

- Защита информации в распределенных информационных системах
- Защита и обработка документов ограниченного доступа
- Комплексные системы защиты информации в правоохранительной сфере
- Управление информационной безопасностью
- Компьютерная экспертиза

3. Объем дисциплины в ЗЕ/академ. час

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 1.

Таблица 1 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№7
1	2	3
Общая трудоемкость дисциплины, ЗЕ/(час)	3/ 108	3/ 108
Из них часов практической подготовки	28	28
Аудиторные занятия, всего час., ***В том числе***	51	51
Лекции (Л), (час)	17	17
Практические/семинарские занятия (ПЗ), (час)	34	34
Лабораторные работы (ЛР), (час)		
Курсовой проект (работа) (КП, КР), (час)		
Экзамен, (час)		

Самостоятельная работа, всего (час)	57	57
Вид промежуточной аттестации: зачет, экзамен, дифференцированный зачет **(Зачет. Экз. Дифф. зач)**	Дифф. Зач.	Дифф. Зач.

4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий

Разделы и темы дисциплины и их трудоемкость приведены в таблице 2.

Таблица 2 – Разделы, темы дисциплины и их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП (час)	СРС (час)
Семестр 7					
Раздел 1. Автоматизированная информационная система как объект защиты	2	4			7
Раздел 2. Требования информационной безопасности АИС	4	12			16
Раздел 3. Методы защиты информации	6	10			16
Раздел 4. Средства защиты информации	5	8			18
Итого в семестре:	17	34			57
Итого:	17	34	0	0	57

4.2. Содержание разделов и тем лекционных занятий

Содержание разделов и тем лекционных занятий приведено в таблице 3.

Таблица 3 - Содержание разделов и тем лекционных занятий

Номер раздела	Название и содержание разделов и тем лекционных занятий
1	Тема 1.1. Архитектура «клиент-сервер» АИС. Тема 1.2. Модели нарушителя и угроз АИС
2	Тема 2.1. Общие требования к построению защищенной АИС. Тема 2.2. Требования к подсистеме аутентификации и управления доступом. Тема 2.3. Требования к подсистемам криптографической защиты информации и антивирусной защиты. Тема 2.4. Требования к подсистемам резервирования /восстановления информации, контроля эталонного состояния информации и рабочей среды. Тема 2.5. Требования к подсистеме управления безопасностью
3	Тема 3.1. Многоуровневая модель защиты информации в АИС на архитектуре «клиент-сервер». Тема 3.2. Методы защиты информации на физическом уровне модели OSI. Тема 3.3. Методы защиты информации на канальном уровне модели OSI. Тема 3.4. Методы защиты информации на сеансовом уровне модели OSI. Тема 3.5. Методы защиты информации на транспортном уровне модели OSI. Тема 3.6. Методы защиты информации на сеансовом уровне модели OSI. Тема 3.7. Методы защиты информации на прикладном уровне модели OSI.
4	Тема 4.1. Средства защиты информации от несанкционированного доступа. Тема 4.2. Средства защиты информации от вредоносного кода. Тема 4.3. Средства защиты информации от межсетевого воздействия. Тема 4.4. Средства криптографической защиты информации.

4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 4.

Таблица 4 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Семестр 7					
1	Требования к построению защищенной АИС и ее элементов	решение ситуационных задач	8	8	2
2	Многоуровневая модель защиты информации в АИС на архитектуре «клиент-сервер»	занятия по моделированию реальных условий	8	8	3
3	Методы защиты информации на уровнях модели OSI	игровое проектирование	10	8	3
4	Средства защиты информации	решение ситуационных задач	8	4	4
		Всего:	34	28	

4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	№ раздела дисциплины
Учебным планом не предусмотрено			

4.5. Курсовое проектирование (работа)

Учебным планом не предусмотрено.

4.6. Самостоятельная работа студентов

Виды самостоятельной работы и ее трудоемкость приведены в таблице 6.

Таблица 6 - Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 7, час
1	2	3
Самостоятельная работа, всего	57	57
Изучение теоретического материала дисциплины (ТО)	37	37
Подготовка к текущему контролю (ТК)	5	5
Домашнее задание (ДЗ)	15	15

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

Учебно-методические материалы для самостоятельной работы студентов указаны в п.п. 8-10.

6. Перечень основной и дополнительной литературы

6.1. Основная литература

Перечень основной литературы приведен в таблице 7.

Таблица 7 – Перечень основной литературы

Шифр	Библиографическая ссылка / URL адрес	Количество экземпляров в библиотеке (кроме электронных экземпляров)
004/М 87-604316-ED	Мошак Н. Н. Защищенные инфотелеком-муникации. 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	

6.2. Дополнительная литература

Перечень дополнительной литературы приведен в таблице 8.

Таблица 8 – Перечень дополнительной литературы

Шифр	Библиографическая ссылка/ URL адрес	Количество экземпляров в библиотеке (кроме электронных экземпляров)
519.6./8 Т 98	Тюрликов А. М. Методы случайного множественного доступа [Текст]: монография /А. М. Тюрликов; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб.: Изд-во ГУАП, 2014. - 300 с.	30
004.7 Б 43	Администрирование в информационных системах: учебное пособие/ М. Н. Беленькая, С. Т. Малиновский, Н. В. Яковенко. - М.: Горячая линия - Телеком, 2011. - 399 с.	10
	Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с. http://znanium.com/catalog.php?bookinfo=423927	
	Оценка относительного ущерба безопасности информационной системы: Монография / Е.А. Дубинин, Ф.Б. Тебуева, В.В. Копытов. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 192 с. http://znanium.com/catalog.php?bookinfo=471787	

7. Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины

Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины

URL адрес	Наименование
	Не предусмотрено

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

8.1.Перечень программного обеспечения

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10 – Перечень программного обеспечения

№ п/п	Наименование
	Не предусмотрено

8.2.Перечень информационно-справочных систем

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11 – Перечень информационно-справочных систем

№ п/п	Наименование
	Не предусмотрено

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Состав материально-технической базы представлен в таблице 12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Лекционная аудитория	
2	Аудитория для проведения практических занятий	

10. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

10.1. Состав фонда оценочных средств приведен в таблице 13

Таблица 13 - Состав фонда оценочных средств для промежуточной аттестации

Вид промежуточной аттестации	Примерный перечень оценочных средств
Дифференцированный зачёт	Список вопросов; Задачи.

10.2. Перечень компетенций, относящихся к дисциплине, и этапы их формирования в процессе освоения образовательной программы приведены в таблице 14.

Таблица 14 – Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Номер семестра	Этапы формирования компетенций по дисциплинам/практикам в процессе освоения ОП
ПК-1 «способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз»	
4	Криминалистика

6	Теория информационной безопасности
6	Теория кодирования
6	Программно-аппаратная защита информации
6	Производственная (эксплуатационная) практика
7	Методология защиты информации
8	Правовая защита информации
8	Технологии защиты от скрытой передачи данных
8	Организационная защита информации
ПК-2 «способность применять технические и программно-аппаратные средства обработки и защиты информации»	
2	Основы программирования
3	Основы программирования
3	Средства вычислительной техники
5	Криптографическая защита информации
5	Организация ЭВМ и вычислительных систем
5	Основы электро-, радиоизмерений
5	Микропроцессорные системы
6	Программно-аппаратная защита информации
6	Системы и сети передачи данных
6	Теория информационной безопасности
6	Криптографическая защита информации
6	Производственная (эксплуатационная) практика
7	Защита компьютерных сетей
7	Техническая защита информации
7	Методология защиты информации
7	Безопасность сетей ЭВМ
8	Правовая защита информации
8	Защита от вредоносных программ
ПК-17 «способность организовывать подготовку и представлять объект информатизации в ходе аттестации на соответствие требованиям государственных и ведомственных нормативных документов»	
6	Теория информационной безопасности
6	Базы данных
7	Безопасность сетей ЭВМ
7	Защита компьютерных сетей
7	Информационное право
7	Базы данных
7	Методология защиты информации
ПК-18 «способность разрабатывать предложения по совершенствованию системы управления безопасностью информации»	
6	Теория информационной безопасности
7	Методология защиты информации
8	Защита информации в распределенных информационных системах
8	Производственная практика
9	Управление информационной безопасностью
10	Производственная преддипломная практика
ПК-19 «способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности»	
4	Основы информационной безопасности
5	Теория информации

6	Теория информационной безопасности
7	Методология защиты информации

10.3. В качестве критериев оценки уровня сформированности (освоения) у обучающихся компетенций применяется шкала модульно–рейтинговой системы университета. В таблице 15 представлена 100–балльная и 4-балльная шкалы для оценки сформированности компетенций.

Таблица 15 –Критерии оценки уровня сформированности компетенций

Оценка компетенции		Характеристика сформированных компетенций
100-балльная шкала	4-балльная шкала	
$85 \le К \le 100$	«отлично» «зачтено»	- обучающийся глубоко и всесторонне усвоил программный материал; - уверенно, логично, последовательно и грамотно его излагает; - опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления; - умело обосновывает и аргументирует выдвигаемые им идеи; - делает выводы и обобщения; - свободно владеет системой специализированных понятий.
$70 \le К \le 84$	«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.
$55 \le К \le 69$	«удовлетво-рительно» «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.
$К \le 54$	«неудовлетво рительно» «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.

10.4. Типовые контрольные задания или иные материалы:

1. Вопросы (задачи) для экзамена (таблица 16).

Таблица 16 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена

	Учебным планом не предусмотрено

2. Вопросы (задачи) для зачета / дифференцированного зачета (таблица 17).

Таблица 17 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифференцированного зачета
1	Общие требования к построению защищенной АИС.
2	Требования к подсистеме аутентификации и управления доступом.
3	Требования к подсистемам криптографической защиты информации и антивирусной защиты.
4	Требования к подсистемам резервирования /восстановления информации, контроля эталонного состояния информации и рабочей среды.
5	Требования к подсистеме управления безопасностью
6	Многоуровневая модель защиты информации в АИС на архитектуре «клиент-сервер».
7	Методы защиты информации на физическом уровне модели OSI.
8	Методы защиты информации на канальном уровне модели OSI.
9	Методы защиты информации на сеансовом уровне модели OSI.
10	Методы защиты информации на транспортном уровне модели OSI.
11	Методы защиты информации на сеансовом уровне модели OSI.
12	Методы защиты информации на прикладном уровне модели OSI.
13	Средства защиты информации от несанкционированного доступа.
14	Средства защиты информации от вредоносного кода.
15	Средства защиты информации от межсетевого воздействия.
16	Средства криптографической защиты информации.

3. Темы и задание для выполнения курсовой работы / выполнения курсового проекта (таблица 18).

Таблица 18 – Примерный перечень тем для выполнения курсовой работы / выполнения курсового проекта

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

4. Вопросы для проведения промежуточной аттестации при тестировании (таблица 19).

Таблица 19 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов
	Не предусмотрено

5. Контрольные и практические задачи / задания по дисциплине (таблица 20).

Таблица 20 – Примерный перечень контрольных и практических задач / заданий

№ п/п	Примерный перечень контрольных и практических задач / заданий
1	Настройка локальных политик безопасности АРМ
2	Настройка групповых политик безопасности АРМ
3	Администрирование и настройка политики безопасности сервера реляционной базы данных MySQL
4	Настройки изолированной программной среды в операционной системе Windows

10.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и / или опыта деятельности, характеризующих этапы формирования компетенций, содержатся в Положениях «О текущем контроле успеваемости и промежуточной аттестации

студентов ГУАП, обучающихся по программы высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП».

11. Методические указания для обучающихся по освоению дисциплины

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

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.

Планируемы результаты при освоении обучающимся 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;

– научится 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. Автоматизированная информационная система как объект защиты

Тема 1.1. Архитектура «клиент-сервер» АИС.

Тема 1.2. Модели нарушителя и угроз АИС

Раздел 2. Требования информационной безопасности АИС

Тема 2.1. Общие требования к построению защищенной АИС.

Тема 2.2. Требования к подсистеме аутентификации и управления доступом.

Тема 2.3. Требования к подсистемам криптографической защиты информации и антивирусной защиты.

Тема 2.4. Требования к подсистемам резервирования /восстановления информации, контроля эталонного состояния информации и рабочей среды.

Тема 2.5. Требования к подсистеме управления безопасностью

Раздел 3. Методы защиты информации

Тема 3.1. Многоуровневая модель защиты информации в АИС на архитектуре «клиент-сервер».

Тема 3.2. Методы защиты информации на физическом уровне модели OSI.

Тема 3.3. Методы защиты информации на канальном уровне модели OSI.

Тема 3.4. Методы защиты информации на сеансовом уровне модели OSI.

Тема 3.5. Методы защиты информации на транспортном уровне модели OSI.

Тема 3.6. Методы защиты информации на сеансовом уровне модели OSI.
Тема 3.7. Методы защиты информации на прикладном уровне модели OSI.
Раздел 4. Средства защиты информации
Тема 4.1. Средства защиты информации от несанкционированного доступа.
Тема 4.2. Средства защиты информации от вредоносного кода.
Тема 4.3. Средства защиты информации от межсетевого воздействия.
Тема 4.4. Средства криптографической защиты информации.

Методические указания для обучающихся по прохождению практических занятий

Практическое занятие является одной из основных форм организации учебного процесса, заключающаяся в выполнении обучающимися под руководством преподавателя комплекса учебных заданий с целью усвоения научно-теоретических основ учебной дисциплины, приобретения умений и навыков, опыта творческой деятельности.

Целью практического занятия для обучающегося является привитие обучающемся умений и навыков практической деятельности по изучаемой дисциплине.

Планируемые результаты при освоении обучающемся практических занятий:

– закрепление, углубление, расширение и детализация знаний при решении конкретных задач;

– развитие познавательных способностей, самостоятельности мышления, творческой активности;

– овладение новыми методами и методиками изучения конкретной учебной дисциплины;

– выработка способности логического осмысления полученных знаний для выполнения заданий;

– обеспечение рационального сочетания коллективной и индивидуальной форм обучения.

Функции практических занятий:

– познавательная;
– развивающая;
– воспитательная.

По характеру выполняемых обучающимся заданий по практическим занятиям подразделяются на:

– ознакомительные, проводимые с целью закрепления и конкретизации изученного теоретического материала;

– аналитические, ставящие своей целью получение новой информации на основе формализованных методов;

– творческие, связанные с получением новой информации путем самостоятельно выбранных подходов к решению задач.

Формы организации практических занятий определяются в соответствии со специфическими особенностями учебной дисциплины и целями обучения. Они могут проводиться:

– в интерактивной форме (решение ситуационных задач, занятия по моделированию реальных условий, деловые игры, игровое проектирование, имитационные занятия, выездные занятия в организации (предприятия), деловая учебная игра, ролевая игра, психологический тренинг, кейс, мозговой штурм, групповые дискуссии);

– в не интерактивной форме (выполнение упражнений, решение типовых задач, решение ситуационных задач и другое).

Методика проведения практического занятия может быть различной, при этом важно достижение общей цели дисциплины.

Требования к проведению практических занятий

Практические занятия носят исследовательский характер и проводятся в следующей последовательности:

- изложение преподавателем теоретических и методических основ исследований;
- обсуждение объекта исследований;
- обсуждение цели и задачи исследований;
- задание и исходные данные для расчетов;
- мозговой штурм и коллективный выбор используемых для решения задачи методов;
- индивидуальная выполнение варианта задания;
- графическое представление полученных результатов;
- мозговой штурм по формирование выводов.

Отчет по практическому занятию представляется индивидуально или группой не более 2 человек в печатном или электронном виде.

Структура отчета включает разделы:

- описание объекта исследований в том числе представление его структуры;
- цели и задачи исследований;
- исходные данные для выполнения индивидуального задания;
- выполнение варианта задания;
- графическое представление полученных результатов;
- выводы.

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 им 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 обучающихся являются учебно-методический материал по дисциплине.

Для развития у студентов навыков самостоятельного овладения теоретическим материалом ряд тем дисциплины на лекционных занятиях дается обзорно, что предполагает их самостоятельное детальное изучение.

Перечень тем для самостоятельного изучения:

- Модели нарушителя и угроз АИС
- Общие требования к построению защищенной АИС.
- Требования к подсистеме аутентификации и управления доступом.
- Требования к подсистемам криптографической защиты информации и антивирусной защиты.
- Требования к подсистемам резервирования /восстановления информации, контроля эталонного состояния информации и рабочей среды.
- Требования к подсистеме управления безопасностью
- Многоуровневая модель защиты информации в АИС на архитектуре «клиент-сервер».
- Методы защиты информации на физическом уровне модели OSI.
- Методы защиты информации на канальном уровне модели OSI.
- Методы защиты информации на сеансовом уровне модели OSI.
- Методы защиты информации на транспортном уровне модели OSI.
- Методы защиты информации на сеансовом уровне модели OSI.

- Методы защиты информации на прикладном уровне модели OSI.
- Средства защиты информации от несанкционированного доступа.
- Средства защиты информации от вредоносного кода.
- Средства защиты информации от межсетевого воздействия.
- Средства криптографической защиты информации.

Методические указания для обучающихся по прохождению промежуточной аттестации

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

Дифференцированный зачет – это форма оценки знаний, полученных обучающимся при изучении дисциплины, при выполнении курсовых проектов, курсовых работ, научно-исследовательских работ и прохождении практик с аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Система оценок при проведении промежуточной аттестации осуществляется в соответствии с требованиями Положений «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программы высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП».

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