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

«Защита компьютерных сетей»
(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.т.н.,доц. 24.06.21 В.А. Мыльников
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 «Защита компьютерных сетей» входит в вариативную часть образовательной программы подготовки обучающихся по специальности «10.05.05 «Безопасность информационных технологий в правоохранительной сфере» специализация «Технологии защиты информации в правоохранительной сфере». Дисциплина реализуется кафедрой №34.

Дисциплина нацелена на формирование у выпускника

профессиональных компетенций:

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

ПК-5 «способность осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного населения»,

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

ПК-29 «способность формировать рабочую техническую документацию с учетом действующих нормативных и методических документов в области безопасности информации»,

ПК-31 «способность принимать участие в создании системы защиты информации на объекте информатизации».

Содержание дисциплины охватывает круг вопросов, связанных с представлением о принципах построения вычислительных сетей, методах организации безопасности в таких сетях и способах аудита. Студент должен знать методы администрирования компьютерных сетей, основные подходы к реализации механизмов безопасности в информационных системах, методы защиты от несанкционированного доступа, способы проектирования компонентов информационных систем, функционирование основных протоколов и сервисов Интернета.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные работы, консультации и самостоятельную работу студента.

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

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часа.

Язык обучения по дисциплине «русский».

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Целью дисциплины «Защита компьютеных сетей» является: формирование знаний, позволяющих применять современные технологии в вычислительных сетях на этапах от проектирования до эксплуатации, обобщение теоретических знаний, на конкретных примерах сред систем и сервисов, формирование у студентов специальных знаний в области управления современными системами и создания программного обеспечения.

В области воспитания личности целью подготовки по данной дисциплине является закрепление общекультурных и профессиональных компетенций для приобретения качеств, необходимых создателю новых технологий, таких как целеустремленность, организованность, трудолюбие, ответственность, гражданственность, коммуникативность и др.

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

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:
ПК-2 «способность применять технические и программно-аппаратные средства обработки и защиты информации»:

знать – значение информации в развитии современного информационного общества;
уметь – выполнять требования к информационной безопасности;
владеть навыками – настройки компонентов информационной системы;
иметь опыт деятельности – в построении безопасных информационных систем и вычислительных сетей.

ПК-5 «способность осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного населения»:

знать – этапы проектирования системы защиты вычислительных сетей;
уметь – проводить системный анализ;
владеть навыками – обследования уже существующих сетей;
иметь опыт деятельности – в поиске взаимосвязей компонентов вычислительных сетей

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

знать - математические методы обработки, анализа и синтеза результатов профессиональных исследований;
уметь - использовать математические методы обработки, анализа и синтеза результатов профессиональных исследований;
владеть навыками - использования математических методов обработки, анализа и синтеза результатов профессиональных исследований;
иметь опыт деятельности – применения на практике математических методов обработки, анализа и синтеза результатов профессиональных исследований

ПК-29 «способность формировать рабочую техническую документацию с учетом действующих нормативных и методических документов в области безопасности информации»:

знать - основные подходы к реализации механизмов безопасности в вычислительных сетях;
уметь - проводить анализ и контроль состояния работающих вычислительных сетей;
владеть навыками – проектирования компонентов вычислительных сетей, проведения аудита состояния безопасности вычислительной сети;
иметь опыт деятельности – в построении безопасной вычислительной сети, принципах, процедурах и службах администрирования вычислительных сетей

ПК-31 «способность принимать участие в создании системы защиты информации на объекте информатизации»:
знать – методы администрирования и контроля;
уметь – проектировать, устанавливать и настраивать службы безопасности, организации доступа, именования и адресации;
владеть навыками – проектирования компонентов компьютерных сетей и проведения аудита состояния безопасности компьютерной сети;
иметь опыт деятельности - принципах, процедурах и службах администрирования вычислительных сетей.

2. Место дисциплины в структуре ОП

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

- Средства вычислительной техники
- Криптографическая защита информации
- Организация ЭВМ и вычислительных систем
- Основы электро-, радиоизмерений
- Микропроцессорные системы
- Программно-аппаратная защита информации
- Системы и сети передачи данных
- Теория информационной безопасности
- Основы информационной безопасности

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

- Комплексные системы защиты информации в правоохранительной сфере
- Информационно-аналитическое обеспечение правоохранительной деятельности
- Защита информации в распределенных информационных системах
- Производственная преддипломная практика

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	4/ 144	4/ 144

дисциплины, ЗЕ/(час)		
Из них часов практической подготовки	34	34
Аудиторные занятия, всего час., ***В том числе***	51	51
лекции (Л), (час)	17	17
Практические/семинарские занятия (ПЗ), (час)		
лабораторные работы (ЛР), (час)	34	34
курсовой проект (работа) (КП, КР), (час)		
Экзамен, (час)	36	36
Самостоятельная работа, всего	57	57
Вид промежуточного контроля: зачет, дифф. зачет, экзамен **(Зачет, Дифф. зач, Экз.)**	Экз.	Экз.

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. Администрированпие вычислительных сетей.	5		8		12
Раздел 2. Защита трафика	4		8		15
Раздел 3. Анализ трафика	4		8		15
Раздел 4. Тестирование на проникновение	4		10		15
Итого в семестре:	17		34		57
Итого:	17	0	34	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	**Администрирование вычислительных сетей** Принципы построения ЛВС. Сетевые сервисы и службы. Сетевое оборудование. Адресация в компьютерных сетях. Стек протоколов TCP/IP. Глобальные сети. Средства администрирования.

	Технология SIEM. Классификация угроз. Стадии проведения сетевой атаки.
2	**Защита трафика** Межсетевые экраны. Брандмауэр Windows. Дистрибутивы для построения межсетевых экранов. Дистрибутивы на основе FreeBSD. Дистрибутивы на основе Linux. Технология IPSec. Технология VPN. Безопасная сеть на основе технологии Infotecs VipNet. ПАК VipNet.
3	**Анализ трафика** Анализаторы трафика. Принципы построения систем обнаружения вторжения. Принципы построения систем предотвращения вторжений.
4	**Тестирование на проникновение** Аудит безопасности. Инструменты для тестирования на проникновение. Защита рабочих станций и серверов. Дистрибутив Kali Linux. Эксплоиты. Эксплуатация уязвимостей с использованием Metasploit.

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)	№ раздела дисципли-ны
Учебным планом не предусмотрено				
		Всего:		

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)	Из них практической подготовки, (час)	№ раздела дисциплины
	Семестр 7			
1	Сетевые утилиты	4	4	1
2	Технология IPSec	4	4	1
3	Утилита IPTables	4	4	2
4	Дистрибутивы для построения межсетевых экранов	4	4	2
5	Анализ трафика	4	4	3
6	Защита трафика	4	4	3
7	Аудит безопасности	4	4	4
8	Эксплуатация уязвимостей с использованием Metasploit	4	4	4
9	Защита рабочих станций и серверов	2	2	4
	Всего:	34	34	

4.5. Курсовое проектирование (работа)

Учебным планом не предусмотрено

4.6. Самостоятельная работа обучающихся

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)	40	40
курсовое проектирование (КП, КР)		
расчетно-графические задания (РГЗ)		
выполнение реферата (Р)		
Подготовка к текущему контролю (ТК)	17	17
домашнее задание (ДЗ)		
контрольные работы заочников (КРЗ)		

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

Учебно-методические материалы для самостоятельной работы обучающихся 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(075) О-54	Олифер, В. Г. Компьютерные сети : Принципы, технологии, протоколы [Текст] : учебное пособие / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - СПб. : ПИТЕР, 2012. - 944 с.	50
http://e.lanbook.com/books/element.php?pl1_id=11484	Агеев, Е.Ю. Основы компьютерных сетевых технологий [Электронный ресурс] : . — Электрон. дан. — М. : ТУСУР (Томский государственный университет систем управления и радиоэлектроники), 2011. — 83 с. — Режим доступа:.	

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)
004.4 К 35	Кенин, А. М. Практическое руководство системного администратора [Текст] / А. М. Кенин. - СПб. : БХВ - Петербург, 2010. - 464 с.	9
http://e.lanbook.com/books/element.php?pl1_id=65915	Никифоров, С.Ф. Введение в сетевые технологии: Элементы применения и администрирования сетей [Электронный ресурс] : учебное пособие. — Электрон. дан. — М. : Финансы и статистика, 2007. — 224 с..	

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
https://webware.biz/?p=3920	Книга «Тестирование на проникновение с Kali Linux» на русском языке
http://ru.docs.kali.org/	Kali Linux Official Documentation

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	Компьютерный класс	

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
Экзамен	Список вопросов; Задания.

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-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-5 «способность осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их	

работоспособного населения»	
3	Средства вычислительной техники
3	Основы электротехники и радиоэлектроники
4	Программирование. Методы и технологии программирования
4	Основы электротехники и радиоэлектроники
5	Микропроцессорные системы
5	Организация ЭВМ и вычислительных систем
5	Основы электро-, радиоизмерений
6	Программно-аппаратная защита информации
6	Системы и сети передачи данных
6	Производственная (эксплуатационная) практика
7	Защита компьютерных сетей
7	Безопасность сетей ЭВМ
8	Противодействие преступлениям в сфере информационных технологий
8	Программирование. Языки программирования
9	Комплексные системы защиты информации в правоохранительной сфере
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-29 «способность формировать рабочую техническую документацию с учетом действующих нормативных и методических документов в области безопасности информации»	
4	Основы информационной безопасности
7	Безопасность сетей ЭВМ
7	Защита компьютерных сетей
7	Распределенные информационные системы
8	Защита и обработка документов ограниченного доступа
9	Компьютерная экспертиза
9	Информационно-аналитическое обеспечение правоохранительной деятельности
9	Технологии защиты электронных платежей
9	Защита банковской информации
9	Технологии защищенного документооборота
ПК-31 «способность принимать участие в создании системы защиты информации на объекте информатизации»	

4	Основы информационной безопасности
4	Производственная (технологическая) практика
5	Криптографическая защита информации
5	Информационно-психологическое обеспечение правоохранительной деятельности
6	Криптографическая защита информации
7	Распределенные информационные системы
7	Защита компьютерных сетей
7	Безопасность сетей ЭВМ
8	Защита информации в распределенных информационных системах
9	Информационно-аналитическое обеспечение правоохранительной деятельности
9	Технологии защиты электронных платежей
9	Защита банковской информации
9	Компьютерная экспертиза
10	Производственная преддипломная практика

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 ≤ 54	«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.

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 зачета / дифференцированного зачета
1	Принципы построения ЛВС. Сетевые сервисы и службы. Сетевое оборудование.
2	Адресация в компьютерных сетях. Стек протоколов TCP/IP. Глобальные сети.
3	Средства администрирования вычислительных сетей.
4	Технология SIEM.
5	Классификация угроз.
6	Стадии проведения сетевой атаки.
7	Понятие и назначение межсетевых экранов.
8	Брандмауэр Windows.
9	Утилита iptables.
10	Дистрибутивы межсетевых экранов на основе FreeBSD.
11	Дистрибутивы межсетевых экранов на основе Linux.
12	Технология IPSec.
13	Технология VPN.
14	Безопасная сеть на основе технологии Infotecs VipNet. ПАК VipNet.
15	Анализаторы трафика.
16	Принципы построения систем обнаружения вторжения.
17	Принципы построения систем предотвращения вторжений.
18	Системы виртуальных ловушек.
19	Аудит безопасности и тестирование на проникновение.
20	Инструменты для тестирования на проникновение.
21	Описание и возможности специализированного дистрибутива Kali Linux.
22	Эксплоиты.
23	Атаки на сервера. Методы защиты.
24	Атаки на рабочие станции. Методы защиты.
25	Платформа Metasploit Framework.

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
	Учебным планом не предусмотрено

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
	Учебным планом не предусмотрено

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

6. Таблица 20 – Примерный перечень контрольных и практических задач / заданий

№ п/п	Примерный перечень контрольных и практических задач / заданий
1	Принципы построения вычислительных сетей.
2	Задачи решаемые администратором сети.
3	Перечень угроз вычислительным сетям
4	Стадии сетевой атаки
5	Место и роль межсетевого экрана в обеспечении сетевой безопасности
6	Задачи не решаемые межсетевым экраном
7	Способы защиты трафика
8	Элементы тестирования на проникновение
9	Защита рабочих станций
10	Защита серверов

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 программам 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 – получение студентами необходимых знаний, умений и навыков в области защиты компьютерных сетей, которые дают представление о возможностях студентов развить и продемонстрировать навыки в области сетевых технологий.

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:

- Изложение лекционного материала;
- Представление теоретического материала преподавателем в виде слайдов;
- Освоение теоретического материала по практическим вопросам;
- Список вопросов по теме для самостоятельной работы студента (Табл.21).

Методические указания для обучающихся по прохождению 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 у 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 (ЛР)

- В задании должно быть четко сформулирована задача, выполняемая в ЛР;
- Описаны входные и выходные данные для проведения ЛР;
- ЛР должна выполняться на основе полученных теоретических знаниях;
- Выполнение ЛР должно осуществляться на основе методических указаний, предоставляемых преподавателем;
- ЛР должна выполняться в специализированном компьютерном классе и может быть доработана студентом в домашних условиях, если позволяет ПО;
- Итогом выполненной ЛР является отчет.

Структура и форма отчета о лабораторной работе

- Постановка задачи;
- Входные и выходные данные;
- Содержание этапов выполнения;
- Обоснование полученного результата (вывод);
- Список используемой литературы.

Требования к оформлению отчета о лабораторной работе

- Лабораторная работа (ЛР) предоставляется в печатном/или электронном виде;
- ЛР должна соответствовать структуре и форме отчета представленной выше;

- ЛР должна иметь титульный лист (ГОСТ 7.32-2001 издания 2008 года) с названием и подписью студента(ов), который(ые) ее сделал(и) и оформил(и);
- Студент должен защитить ЛР. Отметка о защите должна находиться на титульном листе вместе с подписью преподавателя.

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.
Для обучающихся по заочной форме обучения, самостоятельная работа может включать в себя контрольную работу.
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.

Примерный перечень тем для самостоятельного освоения представлен в таблице 21.
Таблица 21 –Примерный перечень тем для самостоятельного изучения

№ п/п	Название темы
1.	Защита рабочих станций с использованием персональных сетевых фильтров.
2.	Организация VPN-сетей. Задачи, решаемые VPN. Туннелирование в VPN.
3.	Электронные сертификаты. Понятие инфраструктуры открытых ключей
4.	Протоколы и средства организации VPN на сетевом уровне. Назначение, область применения, аутентификация и шифрование данных в протоколах SKIP и IPSec
5.	Преимущества технологии терминального доступа. Обеспечение безопасности
6.	Аудит безопасности компьютерных систем. Цели, стандарты, подходы.
7.	Инструментальные средства аудита безопасности компьютерных систем, их возможности и недостатки. Применение инструментальных средств аудита безопасности компьютерных систем.
8.	Службы каталогов. Общие сведения о службах каталогов. Структура каталога LDAP. 14.Система единого входа в сеть на основе протокола Kerberos.
9.	Классификация средств и информационных ресурсов в соответствии со стандартом ISO-17799
10.	Назначение систем обнаружения атак. Классификация систем обнаружения атак. Использование системы обнаружения атак «Snort»

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».

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