

**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ**
**«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)**

Кафедра _____ Защищенных систем связи _____
(полное наименование кафедры)



Регистрационный №_23.05/670-Д

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Этичный хакинг

(наименование дисциплины)

образовательная программа высшего образования

09.04.04 Программная инженерия

(код и наименование направления подготовки / специальности)

магистр

(квалификация)

Программное обеспечение киберфизических систем

(направленность / профиль образовательной программы)

очная форма

(форма обучения)

Санкт-Петербург

Рабочая программа дисциплины составлена на основе требований Федерального государственного образовательного стандарта высшего образования по направлению (специальности) подготовки «09.04.04 Программная инженерия», утвержденного приказом Министерства образования и науки Российской Федерации от 19.09.2017 № 932, и в соответствии с рабочим учебным планом, утвержденным ректором университета.

1. Цели и задачи дисциплины

Целью преподавания дисциплины «Этичный хакинг» является:
изучение методов анализа угроз корпоративной сети

Эта цель достигается путем решения следующих(ей) задач(и):

умение применить различные методы анализа угроз и обнаружения вредоносного ПО

2. Место дисциплины в структуре образовательной программы

Дисциплина «Этичный хакинг» Б1.В.07 относится к части, формируемой участниками образовательных отношений программы магистратуры «09.04.04 Программная инженерия». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как: «Программирование устройств и приложений кибер-физических систем».

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

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Таблица 1

№ п/п	Код компетенции	Наименование компетенции
1	ОПК-4	Способен применять на практике новые научные принципы и методы исследований
2	ПК-5	Способность выполнить постановку новых задач анализа и синтеза новых проектных решений

Индикаторы достижения компетенций

Таблица 2

ОПК-4.1	Знать новые научные принципы и методы исследований
ОПК-4.2	Уметь применять на практике новые научные принципы и методы исследований
ОПК-4.3	Иметь навыки применения новых научных принципов и методов исследования для решения профессиональных задач
ПК-5.1	Знает методы постановки новых задач анализа и синтеза новых проектных решений
ПК-5.2	Умеет использовать методы постановки новых задач анализа и синтеза новых проектных решений
ПК-5.3	Имеет навыки постановки новых задач анализа и синтеза новых проектных решений

4. Объем дисциплины и виды учебной работы

Очная форма обучения

Таблица 3

Вид учебной работы		Всего часов	Семестры
			3
Общая трудоемкость	5 ЗЕТ	180	180

Контактная работа с обучающимися	72.35	72.35
в том числе:		
Лекции	20	20
Практические занятия (ПЗ)	26	26
Лабораторные работы (ЛР)	24	24
Защита контрольной работы		-
Защита курсовой работы		-
Защита курсового проекта		-
Промежуточная аттестация	2.35	2.35
Самостоятельная работа обучающихся (СРС)	74	74
в том числе:		
Курсовая работа		-
Курсовой проект		-
И / или другие виды самостоятельной работы: подготовка к лабораторным работам, практическим занятиям, контрольным работам, изучение теоретического материала	74	74
Подготовка к промежуточной аттестации	33.65	33.65
Вид промежуточной аттестации		Экзамен

5. Содержание дисциплины

5.1. Содержание разделов дисциплины.

Таблица 4

№ п/п	Наименование раздела дисциплины	Содержание раздела	№ семестра		
			очная	очно-заочная	заочная
1	Раздел 1. Сканирование и рекогносцировка в сетевой ИРинфраструктуре	Основные методы идентификации устройств в IP-сети, программное обеспечение для проведения идентификации. Сканирование сетевой инфраструктуры и определение топологии сети	3		
2	Раздел 2. Эксплуатация уязвимостей операционных и SCADAсистем	Основные методы поиска уязвимостей операционных систем (Windows, Linux, MacOS). Методы эксплуатации уязвимостей. Использование п/о rootkits, keylogger. Эксплуатация уязвимостей файловых систем и подсистем ввода/вывода информации. Основы поиска уязвимостей SCADA-систем	3		
3	Раздел 3. Перехват трафика	Основные методы перехвата трафика на канальном и сетевом уровне, в соответствии со стекком протоколов TCP/IP. Эксплуатация уязвимостей типа подмены MAC, IP-адресов. Атаки на ARPпротокол. Основное п/о для эксплуатации уязвимостей такого типа	3		
4	Раздел 4. Отказы в обслуживании	Проведение атак типа «Отказ в обслуживании» и «Распределенный отказ в обслуживании». Основное п/о для проведения атак такого типа. Принципы атак такого типа	3		

5	Раздел 5. Перехват сессий и сетевых соединений	Основные методы поиска уязвимостей в реализации протоколов сетевого и транспортного уровней, в соответствии со стеком протоколов TCP/IP. Методы эксплуатации уязвимостей такого типа. Перехват соединений TCP. Основное п/о для эксплуатации уязвимостей такого типа.	3		
6	Раздел 6. Эксплуатация уязвимостей WEB-сервисов и приложений	Основные методы поиска и эксплуатации уязвимостей WEB-сервисов (HTTP) и WEB-приложений (с использованием языков программирования Java, PHP). Исследование SQL-инъекций.	3		
7	Раздел 7. Поиск и эксплуатация уязвимостей беспроводных сетей, работающих по стандарту 802.11	Основные методы поиска и эксплуатации уязвимостей беспроводных сетей Wi-Fi. Основные уязвимости в протоколах безопасности WEP, WPA/WPA2. П/о для эксплуатации уязвимостей такого типа.	3		
8	Раздел 8. Методы обхода систем предотвращения вторжений и межсетевых экранов	Основные методы поиска и эксплуатации уязвимостей в работе систем предотвращения вторжений и межсетевых экранов. Программное обеспечение, позволяющее эксплуатировать уязвимости такого типа	3		
9	Раздел 9. Использование вирусов, закладок в коде. Переполнение буфера	Основные методы использования вредоносного п/о при проведении анализа уязвимостей инфокоммуникационных систем. Использование ошибок в программном коде для проведения атак типа «Переполнение буфера».	3		
10	Раздел 10. Методы сокрытия деятельности в сети	Основные методы анонимизации присутствия в цифровом пространстве и методы сокрытия деятельности, связанной с сетевой активностью	3		

5.2. Междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами.

Таблица 5

№ п/п	Наименование обеспечиваемых (последующих) дисциплин
1	Блокчейн в сетях связи

5.3. Разделы дисциплин и виды занятий.

Очная форма обучения

Таблица 6

№ п/п	Наименование раздела дисциплины	Лек-ции	Практ. занятия	Лаб. занятия	Семи-нары	СРС	Всего часов
1	Раздел 1. Сканирование и рекогносцировка в сетевой ИРинфраструктуре	2	2	2		8	14

2	Раздел 2. Эксплуатация уязвимостей операционных и SCADA систем	2	2	2		8	14
3	Раздел 3. Перехват трафика	2	4	2		8	16
4	Раздел 4. Отказы в обслуживании	2	2	2		6	12
5	Раздел 5. Перехват сессий и сетевых соединений	2	4	2		6	14
6	Раздел 6. Эксплуатация уязвимостей WEBсервисов и приложений	2	2	2		6	12
7	Раздел 7. Поиск и эксплуатация уязвимостей беспроводных сетей, работающих по стандарту 802.11	2	2	2		8	14
8	Раздел 8. Методы обхода систем предотвращения вторжений и межсетевых экранов	2	2	4		8	16
9	Раздел 9. Использование вирусов, закладок в коде. Переполнение буфера	2	2	2		8	14
10	Раздел 10. Методы сокрытия деятельности в сети	2	4	4		8	18
Итого:		20	26	24	-	74	144

6. Лекции

Очная форма обучения

Таблица 7

№ п/п	Номер раздела	Тема лекции	Всего часов
1	1	Сканирование сетевой инфраструктуры и определение топологии сети	2
2	2	Методы поиска уязвимостей операционных систем (Windows, Linux, MacOS)	2
3	3	Методы перехвата трафика на канальном и сетевом уровне	2
4	4	Проведение атак типа «Отказ в обслуживании» и «Распределенный отказ в обслуживании»	2
5	5	Методы поиска уязвимостей в реализации протоколов сетевого и транспортного уровней	2
6	6	Методы поиска и эксплуатации уязвимостей WEB-сервисов (HTTP) и WEBприложений	2
7	7	Методы поиска и эксплуатации уязвимостей беспроводных сетей WiFi.	2
8	8	Методы поиска и эксплуатации уязвимостей в работе систем предотвращения вторжений и межсетевых экранов	2
9	9	Методы использования вредоносного п/о при проведении анализа уязвимостей инфокоммуникационных систем	2
10	10	Методы анонимизации присутствия в цифровом пространстве и методы сокрытия деятельности	2
Итого:			20

7. Лабораторный практикум

Очная форма обучения

Таблица 8

№ п/п	Номер раздела	Наименование лабораторной работы	Всего часов
1	1	Сканирование и рекогносцировка в аудируемой сети с использованием п/о NSlookup, WHOIS, ping, tracert, NMAP	2
2	2	Тестирование на проникновение инфраструктуры рабочих столов под управлением ОС Windows Server 2012	2
3	3	Перехват трафика с помощью снифферов Wireshark (перенаправления трафика) и прямого подключения к среде передачи	2
4	4	Проведение тестирования аудируемой системы на устойчивость к DDoS-атакам	2
5	5	Перехват TCP-соединений и перенаправления трафика аудируемой организации	2
6	6	Тестирование на проникновение WEB-сервера аудируемой компании с использованием SQL-инъекций	2
7	7	Эксплуатация уязвимостей беспроводной сети 802.11 аудируемой компании	2
8	8	Обход устройств безопасности периметра аудируемой компании	4
9	9	Эксплуатация типа переполнения буфера серверов видеонаблюдения аудируемой компании	2
10	10	Анонимизация сетевого присутствия при проведении аудита сети	4
Итого:			24

8. Практические занятия (семинары)

Очная форма обучения

Таблица 9

№ п/п	Номер раздела	Тема занятия	Всего часов
1	1	Сканирование и рекогносцировка в аудируемой сети с использованием сервисов Bonjour.	2
2	2	Изучение методов и форм хранения паролей в семействе ОС Windows	2
3	3	Принципы перехвата и зацикливания видеопотока	4
4	4	Исследование формирования BOTNET'а для организации DDoS-атак.	2
5	5	Подготовка комплексной инфраструктуры для проведения атаки подмены DNS-сервера	4
6	6	Изучение уязвимостей WEB-сервера аудируемой компании на наличие ошибок и дыр в PHP и Java-коде	2
7	7	Изучение протокола TKIP для идентификации уязвимости и последующей эксплуатации	2
8	8	Изучение механизмов идентификации работы с honeypot'ами	2
9	9	Изучение способов установки вредоносного п/о на конечные станции аудируемой организации	2
10	10	Изучение методов анонимизации сетевого присутствия при проведении аудита сети	4
Итого:			26

9. Примерная тематика курсовых проектов (работ)

Рабочим учебным планом не предусмотрено

10. Самостоятельная работа

Очная форма обучения

Таблица 10

№ п/п	Номер раздела	Содержание самостоятельной работы	Форма контроля	Всего часов
1	1	Использование информации из открытых источников для проведения рекогносцировки в сети	Отчет	8
2	2	Исследование создания keylogger'ов для сбора паролей системы; конфигурация портативных загрузочных томов	Отчет	8
3	3	Исследование механизмов перехвата информации методом фиксации излучения передающих видеокабелей	Отчет	8
4	4	Исследование механизмов организации DoS-атак	Отчет	6
5	5	Конфигурация ложного DNS-сервера	Отчет	6
6	6	Исследование возможности использования ошибок в приложениях WEB-сервисов (Apache)	Отчет	6
7	7	Исследования возможностей эксплуатации уязвимостей в протоколах семейства 802.1x (EAP)	Отчет	8
8	8	Исследование возможностей анонимного сбора информации с помощью п/о Trojan-horses	Отчет	8
9	9	Противодействие механизмам digitalforensics для сокрытия своей деятельности в цифровом пространстве	Отчет	8
10	10	Поиск уязвимостей в стандартных реализациях криптографических протоколов	Отчет	8
Итого:				74

11. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Для самостоятельной работы по дисциплине рекомендовано следующее учебно-методическое обеспечение:

- Положение о самостоятельной работе студентов в Санкт-Петербургском государственном университете телекоммуникаций им. проф. М.А. Бонч-Бруевича;
- рекомендованная основная и дополнительная литература;
- конспект занятий по дисциплине;
- слайды-презентации и другой методический материал, используемый на занятиях;
- методические рекомендации по подготовке письменных работ, требования к их содержанию и оформлению (реферат, эссе, контрольная работа) ;
- фонды оценочных средств;
- методические указания к выполнению лабораторных работ для студентов;

12. Фонд оценочных средств для проведения промежуточной аттестации обучающихся

Фонд оценочных средств разрабатывается в соответствии с локальным актом университета "Положение о фонде оценочных средств" и является приложением (Приложение А) к рабочей программе дисциплины.

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине включает в себя:

- перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы;
- описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;
- типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы;
- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Для каждого результата обучения по дисциплине определяются показатели и критерии оценки сформированности компетенций на различных этапах их формирования, шкалы и процедуры оценивания.

13. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

12.1. Основная литература:

1. Штеренберг, Станислав Игоревич. Технологии программной защиты в интернете : учебное пособие / С. И. Штеренберг, В. Е. Морозов, В. И. Андрианов ; рец.: В. А. Васильев, Н. Н. Бабин ; Федеральное агентство связи, Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования "Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича". - СПб. : СПбГУТ. Ч. 1. - 2015. - 60 с. : ил. - ISBN 978-5-89160-126-0 : 322.40 р.
2. Штеренберг, Станислав Игоревич. Технологии программной защиты в интернете : учебное пособие / С. И. Штеренберг, В. Е. Морозов, В. И. Андрианов ; рец.: В. А. Васильев, Н. Н. Бабин ; Федеральное агентство связи, Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования "Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича". - СПб. : СПбГУТ. Ч. 2. - 2015. - 76 с. : ил. - ISBN 978-5-89160-126-0 : 408.37 р.

12.2. Дополнительная литература:

1. Компьютерные вирусы : метод. указ. к лаб. работам / В. И. Андрианов [и др.] ; рец. С. Е. Душин ; Федер. агентство связи, Федер. гос. образовательное бюджет. учреждение высш. проф. образования "С.-Петербур. гос. ун-т телекоммуникаций им. проф. М. А. Бонч-Бруевича". - СПб. : СПбГУТ, 2011. - 19 с. - Библиогр.: с.17. - (в обл.) : 8.75 р. - Текст : непосредственный.

14. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

- www.sut.ru
- lib.spbgut.ru/jirbis2_spbgut

15. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем.

15.1. Программное обеспечение дисциплины:

- Cisco Packet Tracer
- GNU Assembler
- Linux
- Maxima
- NetBeans
- Open JDK
- Oracle VM VirtualBox
- SciLab
- Visual Studio Community
- Windows ИКСС
- ИКБ (Интегрированный комплекс безопасности) КОДОС
- Интерпретатор Python 3
- Комплект КОДОС-ВИДЕОСЕТЬ 4/25

15.2. Информационно-справочные системы:

- ЭБС iBooks (<https://ibooks.ru>)
- ЭБС Лань (<https://e.lanbook.com/>)
- ЭБС СПбГУТ (<http://lib.spbgut.ru>)

16. Методические указания для обучающихся по освоению дисциплины

15.1. Планирование и организация времени, необходимого для изучения дисциплины

Важным условием успешного освоения дисциплины «Этичный хакинг» является создание системы правильной организации труда, позволяющей распределить

учебную нагрузку равномерно в соответствии с графиком образовательного процесса. Большую помощь в этом может оказать составление плана работы на семестр, месяц, неделю, день. Его наличие позволит подчинить свободное время целям учебы, трудиться более успешно и эффективно. Нужно осуществлять самоконтроль, который является необходимым условием успешной учебы. Все задания, включая вынесенные на самостоятельную работу, рекомендуется выполнять непосредственно после соответствующего аудиторного занятия (лекции, практического занятия), что способствует лучшему усвоению материала, позволяет своевременно выявить и устранить «пробелы» в знаниях, систематизировать ранее пройденный материал, на его основе приступить к овладению новыми знаниями и навыками.

Система университетского обучения основывается на рациональном сочетании нескольких видов учебных занятий (в первую очередь, лекций и практических занятий), работа на которых обладает определенной спецификой.

15.2. Подготовка к лекциям

Знакомство с дисциплиной происходит уже на первой лекции, где от студента требуется не просто внимание, но и самостоятельное оформление конспекта. При работе с конспектом лекций необходимо учитывать тот фактор, что одни лекции дают ответы на конкретные вопросы темы, другие – лишь выявляют взаимосвязи между явлениями, помогая студенту понять глубинные процессы развития изучаемого предмета, как в истории, так и в настоящее время.

Конспектирование лекций – сложный вид вузовской аудиторной работы, предполагающий интенсивную умственную деятельность студента. Конспект является полезным тогда, когда записано самое существенное и сделано это самим обучающимся. Не надо стремиться записать дословно всю лекцию. Такое «конспектирование» приносит больше вреда, чем пользы. Целесообразно вначале понять основную мысль, излагаемую лектором, а затем записать ее. Желательно запись осуществлять на одной странице листа или оставляя поля, на которых позднее, при самостоятельной работе с конспектом, можно сделать дополнительные записи, отметить непонятные места.

Конспект лекции лучше подразделять на пункты, соблюдая красную строку. Этому в большой степени будут способствовать вопросы плана лекции, предложенные преподавателям. Следует обращать внимание на акценты, выводы, которые делает лектор, отмечая наиболее важные моменты в лекционном материале замечаниями «важно», «хорошо запомнить» и т.п. Можно делать это и с помощью разноцветных маркеров или ручек, подчеркивая термины и определения.

Целесообразно разработать собственную систему сокращений, аббревиатур и символов. Однако при дальнейшей работе с конспектом символы лучше заменить обычными словами для быстрого зрительного восприятия текста. Работая над конспектом лекций, всегда необходимо использовать не только учебник, но и ту литературу, которую дополнительно рекомендовал лектор. Именно такая серьезная, кропотливая работа с лекционным материалом позволит глубоко овладеть теоретическим материалом.

15.3. Подготовка к практическим занятиям

Тщательное продумывание и изучение вопросов плана основывается на проработке пройденного материала (материала лекций, практических занятий), а затем изучения обязательной и дополнительной литературы, рекомендованной к данной теме.

Результат такой работы должен проявиться в способности студента свободно ответить на теоретические вопросы практикума, его выступлении и участии в коллективном обсуждении вопросов изучаемой темы, правильном выполнении практических заданий и контрольных работ.

Необходимо понимать, что невозможно во время аудиторных занятий изложить весь материал из-за лимита аудиторных часов, и при изучении дисциплины недостаточно конспектов занятий. Поэтому самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов свое отношение к конкретной проблеме.

15.4. Рекомендации по работе с литературой

Работу с литературой целесообразно начать с изучения общих работ по теме, а также учебников и учебных пособий. Далее рекомендуется перейти к анализу монографий и статей, рассматривающих отдельные аспекты проблем, изучаемых в рамках курса, а также официальных материалов и неопубликованных документов (научно-исследовательские работы, диссертации), в которых могут содержаться основные вопросы изучаемой проблемы.

Работу с источниками надо начинать с ознакомительного чтения, т.е. просмотреть текст, выделяя его структурные единицы. При ознакомительном чтении закладками отмечаются те страницы, которые требуют более внимательного изучения. В зависимости от результатов ознакомительного чтения выбирается дальнейший способ работы с источником. Если для разрешения поставленной задачи требуется изучение некоторых фрагментов текста, то используется метод выборочного чтения. Если в книге нет подробного оглавления, следует обратить внимание ученика на предметные и именные указатели.

Избранные фрагменты или весь текст (если он целиком имеет отношение к теме) требуют вдумчивого, неторопливого чтения с «мысленной проработкой» материала. Такое чтение предполагает выделение: 1) главного в тексте; 2) основных аргументов; 3) выводов. Особое внимание следует обратить на то, вытекает тезис из аргументов или нет. Необходимо также проанализировать, какие из утверждений автора носят проблематичный, гипотетический характер и уловить скрытые вопросы.

Понятно, что умение таким образом работать с текстом приходит далеко не сразу. Наилучший способ научиться выделять главное в тексте, улавливать проблематичный характер утверждений, давать оценку авторской позиции – это сравнительное чтение, в ходе которого студент знакомится с различными мнениями по одному и тому же вопросу, сравнивает весомость и доказательность аргументов сторон и делает вывод о наибольшей убедительности той или иной позиции.

Если в литературе встречаются разные точки зрения по тому или иному вопросу

из-за сложности прошедших событий и правовых явлений, нельзя их отвергать, не разобравшись. При наличии расхождений между авторами необходимо найти рациональное зерно у каждого из них, что позволит глубже усвоить предмет изучения и более критично оценивать изучаемые вопросы. Знакомясь с особыми позициями авторов, нужно определять их схожие суждения, аргументы, выводы, а затем сравнивать их между собой и применять из них ту, которая более убедительна.

Следующим этапом работы с литературными источниками является создание конспектов, фиксирующих основные тезисы и аргументы. Можно делать записи на отдельных листах, которые потом легко систематизировать по отдельным темам изучаемого курса. Другой способ – это ведение тематических тетрадей-конспектов по одной какой-либо теме. Большие специальные работы монографического характера целесообразно конспектировать в отдельных тетрадях. Здесь важно вспомнить, что конспекты пишутся на одной стороне листа, с полями и достаточным для исправления и ремарок межстрочным расстоянием (эти правила соблюдаются для удобства редактирования). Если в конспектах приводятся цитаты, то непременно должно быть дано указание на источник (автор, название, выходные данные, № страницы). Впоследствии эта информация может быть использована при написании текста реферата или другого задания.

Таким образом, при работе с источниками и литературой важно уметь:

- сопоставлять, сравнивать, классифицировать, группировать, систематизировать информацию в соответствии с определенной учебной задачей;
- обобщать полученную информацию, оценивать прослушанное и прочитанное;
- фиксировать основное содержание сообщений; формулировать, устно и письменно, основную идею сообщения; составлять план, формулировать тезисы;
- готовить и презентовать развернутые сообщения типа доклада;
- работать в разных режимах (индивидуально, в паре, в группе), взаимодействуя друг с другом;
- пользоваться реферативными и справочными материалами;
- контролировать свои действия и действия своих товарищей, объективно оценивать свои действия;
- обращаться за помощью, дополнительными разъяснениями к преподавателю, другим студентам;
- пользоваться лингвистической или контекстуальной догадкой, словарями различного характера, различного рода подсказками, опорами в тексте (ключевые слова, структура текста, предваряющая информация и др.);
- использовать при говорении и письме перифраз, синонимичные средства, слова-описания общих понятий, разъяснения, примеры, толкования, «словотворчество»
- повторять или перефразировать реплику собеседника в подтверждении понимания его высказывания или вопроса;
- обратиться за помощью к собеседнику (уточнить вопрос, переспросить и др.);
- использовать мимику, жесты (вообще и в тех случаях, когда языковых средств не хватает для выражения тех или иных коммуникативных намерений).

15.5. Подготовка к промежуточной аттестации

При подготовке к промежуточной аттестации целесообразно:

- внимательно изучить перечень вопросов и определить, в каких источниках

- находятся сведения, необходимые для ответа на них;
- внимательно прочитать рекомендованную литературу;
 - составить краткие конспекты ответов (планы ответов).

17. Материально-техническое обеспечение дисциплины

Таблица 11

№ п/п	Наименование специализированных аудиторий и лабораторий	Наименование оборудования
1	Лекционная аудитория	Аудио-видео комплекс
2	Аудитории для проведения групповых и практических занятий	Аудио-видео комплекс
3	Компьютерный класс	Персональные компьютеры
4	Аудитория для курсового и дипломного проектирования	Персональные компьютеры
5	Аудитория для самостоятельной работы	Компьютерная техника
6	Читальный зал	Персональные компьютеры

Лист изменений № 1 от 9 января 2020 г

Рабочая программа дисциплины
«**Этичный хакинг**»

Код и наименование направления подготовки/специальности:

09.04.04 Программная инженерия

Направленность/профиль образовательной программы:

Программное обеспечение кибер-физических систем

Из п. 14.2 Информационно-справочные системы исключить с 08.01.2020 г.
строку: ЭБС IPRbooks (<http://www.iprbookshop.ru>)

Основание: прекращение контракта № 4784/19 от 25.01.2019 г. на
предоставление доступа к электронно-библиотечной системе IPRbooks.

Внесенные изменения утверждаю:

Начальник УМУ _____ Л.А. Васильева