

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)

СПбГУТ))

Документ подписан простой  
электронной подписью

Сертификат: 009b47d8b89b08d0f6  
Владелец: Киричек Руслан Валентинович  
Действителен с 13.02.2023 по 12.02.2028



УТВЕРЖДАЮ

А.В. Абилов

06 2023

Регистрационный №\_23.05/265-Д

## РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита облачных вычислений и телекоммуникаций

(наименование дисциплины)

образовательная программа высшего образования

10.04.01 Информационная безопасность

(код и наименование направления подготовки / специальности)

магистр

(квалификация)

Безопасность компьютерных 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 «10.04.01 Информационная безопасность», утвержденного приказом Министерства образования и науки Российской Федерации от 26.11.2020 № 1455, и в соответствии с рабочим учебным планом, утвержденным ректором университета.

## 1. Цели и задачи дисциплины

Целью преподавания дисциплины «Защита облачных вычислений и телекоммуникаций» является:

изучение принципов построения программно-конфигурируемых сетей, защиты облачных вычислений, принципов работы гипервизора.

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

умение настраивать программно-конфигурируемые сети, облачную инфраструктуру

## 2. Место дисциплины в структуре образовательной программы

Дисциплина «Защита облачных вычислений и телекоммуникаций» Б1.В.01 относится к части, формируемой участниками образовательных отношений программы магистратуры «10.04.01 Информационная безопасность». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как: «Управление информационной безопасностью».

## 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	ПК-1	Проведение контрольных проверок работоспособности программно-аппаратных средств защиты информации
2	ПК-4	Разработка требований по защите компьютерных сетей и систем
3	ПК-5	Разработка средств защиты информации
4	ПК-8	Проведение анализа безопасности компьютерных систем
5	УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий
6	УК-4	Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия
7	УК-5	Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия

### Индикаторы достижения компетенций

Таблица 2

ПК-1.1	Знать: - основные методы проверки работоспособности программно-аппаратных средств защиты информации
ПК-1.2	Уметь: - проводить контрольные проверки работоспособности программно-аппаратных средств защиты информации
ПК-1.3	Владеть: - навыками организации контрольных проверок работоспособности программно-аппаратных средств защиты информации
ПК-4.1	Знать: - основные протоколы и методы защиты компьютерных сетей и систем
ПК-4.2	Уметь: - разрабатывать требования по защите компьютерных сетей и систем

ПК-4.3	Владеть: - навыками настройки средств защиты компьютерных сетей и систем
ПК-5.1	Знать: - основные средства обеспечения защиты информации
ПК-5.2	Уметь: - разрабатывать средства защиты информации
ПК-5.3	Владеть: - навыками настройки средств защиты информации
ПК-8.1	Знать: - основные методы обеспечения безопасности компьютерных систем
ПК-8.2	Уметь: - проводить анализ безопасности компьютерных систем
ПК-8.3	Владеть: - навыками настройки функций безопасности компьютерных систем
УК-1.1	Знать: - методы системного и критического анализа; - методики разработки стратегии действий для выявления и решения проблемной ситуации
УК-1.2	Уметь: - применять методы системного подхода и критического анализа проблемных ситуаций; - разрабатывать стратегию действий, принимать конкретные решения для ее реализации
УК-1.3	Владеть: - методологией системного и критического анализа проблемных ситуаций; - методиками постановки цели, определения способов ее достижения, разработки стратегий действий
УК-4.1	Знать: - правила и закономерности личной и деловой устной и письменной коммуникации; - современные коммуникативные технологии на русском и иностранном языках; - существующие профессиональные сообщества для профессионального взаимодействия
УК-4.2	Уметь: - применять на практике коммуникативные технологии, методы и способы делового общения для академического и профессионального взаимодействия
УК-4.3	Владеть: - методикой межличностного делового общения на русском и иностранном языках, с применением профессиональных языковых форм, средств и современных коммуникативных технологий
УК-5.1	Знать: - закономерности и особенности социально-исторического развития различных культур; - особенности межкультурного разнообразия общества; - правила и технологии эффективного межкультурного взаимодействия
УК-5.2	Уметь: - понимать и толерантно воспринимать межкультурное разнообразие общества; - анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия
УК-5.3	Владеть: - методами и навыками эффективного межкультурного взаимодействия

#### 4. Объем дисциплины и виды учебной работы

Очная форма обучения

Таблица 3

Вид учебной работы	Всего часов	Семестры	
		1	2
Общая трудоемкость	7 ЗЕТ	252	252
<b>Контактная работа с обучающимися</b>	110.35	110.35	
в том числе:			
Лекции	32	32	
Практические занятия (ПЗ)	38	38	
Лабораторные работы (ЛР)	36	36	
Задача контрольной работы		-	
Задача курсовой работы	2	2	
Задача курсового проекта		-	
Промежуточная аттестация	2.35	2.35	
<b>Самостоятельная работа обучающихся (СРС)</b>	108	108	
в том числе:			
Курсовая работа	20	20	

Курсовой проект		-
И / или другие виды самостоятельной работы: подготовка к лабораторным работам, практическим занятиям, контрольным работам, изучение теоретического материала	88	88
Подготовка к промежуточной аттестации	33.65	33.65
<b>Вид промежуточной аттестации</b>		Экзамен

## 5. Содержание дисциплины

### 5.1. Содержание разделов дисциплины.

Таблица 4

№ п/п	Наименование раздела дисциплины	Содержание раздела	№ семестра		
			очно- очная	заоч- ная	заоч- ная
1	Раздел 1. Введение в сети следующего поколения	Рассматривается переход на сети будущего. Проведено сравнение существующих сетей и сетей будущего.	2		
2	Раздел 2. Безопасность и защита в облачных вычислениях	Общие понятия облачных вычислений, проблемы обеспечения безопасности облачных вычислений, методология облачных вычислений	2		
3	Раздел 3. Виртуализация: Проблемы. Угрозы. Решения.	Проблемы виртуализации. Свойства и подходы в виртуализации, угрозы, решения.	2		
4	Раздел 4. Принципы SDN. Протокол Openflow.	Программно-конфигурируемые сети, структура контроллера SDN, примеры конфигурации на решении компании Cisco Systems. Рассматриваются принципы конфигурирования протокола OpenFlow.	2		
5	Раздел 5. Виртуализация сетей	Принципы организации виртуальных сетей (на примере vSwitch от VMware), overlay сети.	2		
6	Раздел 6. Виртуальные частные сети. Сетевой уровень. Транспортный уровень (протокол SSL/TLS)	Рассматриваются все современные методы создания VPN, включая такие методы, как: IPsecVTI, динамические VTI, GETVPN, DMVPN, FlexVPN. Рассматриваются структуры протоколов IPsec, IKEv.1 и v.2, приведены сравнительные характеристики всех современных методов построения VPN. Рассматриваются протоколы построения шифрованных туннелей трафика SSL/TLS. Приводятся основные уязвимости протоколов и способы борьбы с ними.	2		
7	Раздел 7. Защита контроллера SDN	Рассматриваются принципы организации защиты SDN контроллера, на примере компании Cisco Systems.	2		
8	Раздел 8. Системы детекции/предотвращения вторжений и аномалий	Рассматриваются системы предотвращения вторжений и аномалий (на примере ПО с открытым исходным кодом - Snort)	2		
9	Раздел 9. Защита OpenStack	Рассматривается комплекс проектов свободного программного обеспечения, который может быть использован для создания инфраструктурных облачных сервисов и облачных хранилищ, как публичных, так и частных	2		
10	Раздел 10. Настройка продвинутого NAT, фаервола следующего поколения	Приводятся конфигурации и принцип действия фаерволов следующего поколения (NGFW)	2		

11	Раздел 11. Конфиденциальность облачных вычислений. Целостность облачных вычислений	Приводятся основные угрозы и стратегии защиты облачных вычислений. Рассматриваются основные угрозы целостности данных и методы защиты от угроз в облачных вычислениях.	2		
----	--	--	---	--	--

5.2. Междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами.

«Защита облачных вычислений и телекоммуникаций» является дисциплиной, завершающей теоретическое обучение по программе 10.04.01 Информационная безопасность

5.3. Разделы дисциплин и виды занятий.

### Очная форма обучения

Таблица 5

№ п/п	Наименование раздела дисциплины	Лек-ции	Практ. занятия	Лаб. занятия	Семи-нары	СРС	Всего часов
1	Раздел 1. Введение в сети следующего поколения	2	6			10	18
2	Раздел 2. Безопасность и защита в облачных вычислениях	2	4	6		10	22
3	Раздел 3. Виртуализация: Проблемы. Угрозы. Решения.	4	4	4		10	22
4	Раздел 4. Принципы SDN. Протокол Openflow.	4	8			5	17
5	Раздел 5. Виртуализация сетей	2	4	6		5	17
6	Раздел 6. Виртуальные частные сети. Сетевой уровень. Транспортный уровень (протокол SSL/TLS)	6	4	6		9	25
7	Раздел 7. Защита контроллера SDN	2	4			9	15
8	Раздел 8. Системы детекции/предотвращения вторжений и аномалий	2	4			10	16
9	Раздел 9. Защита OpenStack	2		4		10	16
10	Раздел 10. Настройка продвинутого NAT, фаервола следующего поколения	2		6		5	13
11	Раздел 11. Конфиденциальность облачных вычислений. Целостность облачных вычислений	4		4		5	13
Итого:		32	38	36	-	88	194

## 6. Лекции

### Очная форма обучения

Таблица 6

№ п/п	Номер раздела	Тема лекции	Всего часов
1	1	Переход на сети следующего поколения.	2
2	2	Проблемы обеспечения безопасности облачных вычислений	2
3	3	Проблемы виртуализации	2
4	3	Решение угроз виртуализации.	2
5	4	Программно-конфигурируемые сети	2
6	4	Принципы конфигурирования протокола OpenFlow	2
7	5	Организация виртуальных сетей	2
8	6	Современные методы создания VPN	2
9	6	Структуры протоколов IPsec, IKEv.1 и др.	2
10	6	Протоколы построения шифрованных туннелей трафика SSL/TLS	2
11	7	Организации защиты SDN контроллера	2
12	8	Системы предотвращения вторжений и аномалий	2
13	9	Защита OpenStack	2
14	10	Конфигурации и принцип действия фаерволов следующего поколения (NGFW)	2
15	11	Угрозы и стратегии защиты облачных вычислений	2
16	11	Угрозы целостности данных и методы защиты от угроз в облачных вычислениях.	2
			Итого: 32

## 7. Лабораторный практикум

Очная форма обучения

Таблица 7

№ п/п	Номер раздела	Наименование лабораторной работы	Всего часов
1	2	Установка гипервизора и виртуальных машин Ubuntu, MS Windows, MS Windows Server	6
2	3	Создание виртуальной компьютерной сети. Сравнение с реальными сетями	4
3	5	Создание подключения к удаленной сети. Исследование протоколов SSL/TLS	6
4	6	Настройка и запуск IPS Snort	6
5	9	Доступность – атаки и методы защиты в облаке	4
6	10	Настройка продвинутого NAT	6
7	11	Конфиденциальность и целостность – атаки и методы защиты данных в облаке	4
			Итого: 36

## 8. Практические занятия (семинары)

Очная форма обучения

Таблица 8

№ п/п	Номер раздела	Тема занятия	Всего часов
1	1	Установка контроллера OpenFlow. Использование виртуального коммутатора, внедрение openvswitch	4

2	1	Безопасность в виртуализации	2
3	2	Настройка DMVPN на виртуальных маршрутизаторах	4
4	3	Тюнинг и создание собственной сигнатуры для IPS Snort	4
5	4	Настройка OpenStack	4
6	4	Защита контроллера SDN	4
7	5	Конфигурирование средств защиты OpenStack	4
8	6	Настройка виртуального фаервола CiscovASA	4
9	7	Конфиденциальность и целостность – атаки и методы защиты данных в облаке	4
10	8	Доступность – атаки и методы защиты в облаке	4
Итого:			38

## 9. Примерная тематика курсовых проектов (работ)

Учебным планом предусмотрена курсовая работа.

### Подготовка к написанию курсовой работы.

Курсовая работа направлена на закрепление теоретических знаний путем решения конкретной практической задачи по изучаемой дисциплине.

Подбор литературы осуществляется студентом самостоятельно, с учетом рекомендованного перечня. Изучение литературы следует начинать с учебников и учебных пособий, а также рекомендуемых источников к планам семинарских и практических занятий.

План курсовой работы должен состоять из введения, 3 глав и 2-4 вопросов (пунктов) в основной части, заключения, списка литературы и приложений. Формулировки пунктов плана определяются целевой направленностью работы, исходя из её задач.

В процессе написания курсовой работы студент должен разобраться в теоретических вопросах избранной темы, самостоятельно проанализировать практический материал, разобрать и обосновать практические предложения.

В установленные кафедрой сроки законченная курсовая работа представляется на проверку преподавателю. Преподаватель, проверив работу, может возвратить ее для доработки вместе с письменными замечаниями. Студент должен устранить полученные замечания в установленный срок, после чего работа окончательно оценивается.

Таблица 9

№ п/п	Тема курсового проекта (работы)
1	Защита контроллера SDN

## 10. Самостоятельная работа

### Очная форма обучения

Таблица 10

№ п/п	Номер раздела	Содержание самостоятельной работы	Форма контроля	Всего часов
1	1	Установка контроллера OpenFlow. Использование виртуального коммутатора, внедрение openvswitch	отчёт	10

2	2	Настройка DMVPN на виртуальных маршрутизаторах	отчёт	10
3	3	Тюнинг и создание собственной сигнатуры для IPS Snort	отчёт	10
4	4	Настройка OpenStack	отчёт	5
5	5	Конфигурирование средств защиты OpenStack	отчёт	5
6	6	Настройка виртуального фаервола Cisco ASA	отчёт	9
7	7	Конфиденциальность и целостность – атаки и методы защиты данных в облаке	отчёт	9
8	8	Безопасность в виртуализации	отчёт	10
9	9	Доступность – атаки и методы защиты в облаке	отчёт	10
10	10	Создание виртуальной компьютерной сети. Сравнение с реальными сетями	отчёт	5
11	11	Установка гипервизора и виртуальных машин Ubuntu, MS Windows, MS Windows Server	отчёт	5
Итого:				88

## **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;
- методические рекомендации по подготовке и защите курсовой работы (проекта).

## **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 освоений дисциплины**

#### **12.1. Основная литература:**

##### **1. Ушаков, Игорь Александрович.**

Advanced Network & Cloud Security : [Электронный ресурс] : учебное пособие / И. А. Ушаков, А. В. Красов ; рец.: С. Е. Душин, Л. Б. Бузюков ; Федер. агентство связи, Федеральное государственное бюджетное образовательное учреждение высшего образования "Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича". - СПб. : СПбГУТ, 2017. - 55 р. : ил. - 321.00 р.

##### **2. Клементьев, И. П.**

Введение в облачные вычисления : [Электронный ресурс] : учебное пособие / И. П. Клементьев, В. А. Устинов. - 2-е изд. - М. : ИНТУИТ, 2016. - 310 с. - URL: <https://e.lanbook.com/book/100686>. - Б. ц. Книга из коллекции ИНТУИТ - Информатика

#### **12.2. Дополнительная литература:**

##### **1. Риз, Дж.**

Облачные вычисления (Cloud Application Architectures) : [Электронный ресурс] / Дж. Риз. - СПб. : БХВ-Петербург, 2011. - 288 с. : ил. - URL: <http://ibooks.ru/reading.php?productId=26340>. - ISBN 978-5-9775-0630-4 : Б. ц.

##### **2. Савельев, А. О.**

Решения Microsoft для виртуализации ИТ-инфраструктуры предприятий : [Электронный ресурс] : учебное пособие / А. О. Савельев. - 2-е изд. - М. : ИНТУИТ, 2016. - 284 с. - URL: <https://e.lanbook.com/book/100484>. - Б. ц. Книга из коллекции ИНТУИТ - Информатика

##### **3. Surmacz, Tomasz.**

Cyber Security for Next Generation Experts : научное издание / Т. Surmacz, А. Carlsson. - [S. l.] : Karlskrona, 2018. - 209 р. : ил., цв. ил. - ISBN 978-91-7295-962-0 : 800.00 р. - Текст : непосредственный. Перевод заглавия: Кибербезопасность для экспертов следующего поколения

## **14. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»**

- [www.sut.ru](http://www.sut.ru)
- [lib.spbgut.ru/jirbis2\\_spbgut](http://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:**

- Linux
- Oracle VM VirtualBox
- Windows ИКСС

### **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 «Защита облачных вычислений и телекоммуникаций» 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 информации 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  
**«Защита облачных вычислений и телекоммуникаций»**

Код и наименование направления подготовки/специальности:

**10.04.01 Информационная безопасность**

Направленность/профиль образовательной программы:

**Безопасность компьютерных систем**

---

Из п. 14.2 Информационно-справочные системы исключить с 08.01.2020 г.  
стороку: 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