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
Первый проректор – проректор по учебной работе
_____ А.В. Абилов
«23» 06 2023 г.

Регистрационный №_23.05/269-Д

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Управление информационной безопасностью
(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 «Управление информационной безопасностью» является:

изучение вопросов управления информационной безопасностью. Дисциплина «Управление информационной безопасностью» должна обеспечивать формирование фундамента подготовки будущих специалистов в области формирования моделей угроз, оценки рисков информационных инфокоммуникационных систем, формирование адекватных методов и средств обеспечения информационной безопасности, а также, создавать необходимую базу для успешного овладения последующими специальными дисциплинами учебного плана. Она должна способствовать развитию творческих способностей студентов, умению формулировать и решать задачи изучаемой специальности, умению творчески применять и самостоятельно повышать свои знания.

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

на основе фундаментализации, интенсификации и индивидуализации процесса обучения путём внедрения и эффективного использования достижений современного менеджмента в области информационной безопасности на основе национальных и мировых стандартов. В результате изучения дисциплины у студентов должны сформироваться знания, умения и навыки, позволяющие проводить самостоятельный анализ рисков и угроз возникающих в процессе деятельности компаний инфокоммуникационого профиля и операторов связи.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Управление информационной безопасностью» Б1.О.03 относится к обязательной части программы магистратуры «10.04.01 Информационная безопасность».

Изучение дисциплины «Управление информационной безопасностью» основывается на базе знаний, умений и компетенций, полученных студентами на предыдущем уровне образования.

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-2	Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;
2	ОПК-3	Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;
3	ПК-3	Формирование политик информационной безопасности
4	ПК-4	Разработка требований по защите компьютерных сетей и систем
5	ПК-8	Проведение анализа безопасности компьютерных систем

6	ПК-9	Проведение экспертизы при расследовании компьютерных преступлений и инцидентов
7	УК-3	Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели

Индикаторы достижения компетенций

Таблица 2

ОПК-2.1	Знать: - типовые технические проекты системы (подсистемы либо компонента системы) обеспечения информационной безопасности
ОПК-2.2	Уметь: - разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности
ОПК-2.3	Владеть: - навыками проектирования системы (подсистемы либо компонента системы) обеспечения информационной безопасности
ОПК-3.1	Знать: - организационно-распорядительных документов по обеспечению информационной безопасности
ОПК-3.2	Уметь: - разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности
ОПК-3.3	Владеть: - навыками разработки проектов организационно-распорядительных документов по обеспечению информационной безопасности
ПК-3.1	Знакть: - основные политики информационной безопасности
ПК-3.2	Уметь: - формировать политики информационной безопасности
ПК-3.3	Владеть: - навыками формироватния политики информационной безопасности
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-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
ПК-9.1	Знать: - основные методы проведения экспертизы при расследовании компьютерных преступлений и инцидентов
ПК-9.2	Уметь: - проводить экспертизы при расследовании компьютерных преступлений и инцидентов
ПК-9.3	Владеть: - навыками проведения расследований инцидентов и компьютерных преступлений
УК-3.1	Знать: - методики формирования команд; - методы эффективного руководства коллективами; - основные теории лидерства и стили руководства
УК-3.2	Уметь: - разрабатывать план групповых и организационных коммуникаций при подготовке и выполнении проекта; - сформулировать задачи членам команды для достижения поставленной цели; - разрабатывать командную стратегию; - применять эффективные стили руководства командой для достижения поставленной цели
УК-3.3	Владеть: - умением анализировать, проектировать и организовывать межличностные, групповые и организационные коммуникации в команде для достижения поставленной цели; - методами организации и управления коллективом

4. Объем дисциплины и виды учебной работы

Очная форма обучения

Таблица 3

Вид учебной работы	**Всего часов**	**Семестры**
		1

Общая трудоемкость	5 ЗЕТ	180	180
Контактная работа с обучающимися		68.35	68.35
в том числе:			
Лекции		26	26
Практические занятия (ПЗ)		22	22
Лабораторные работы (ЛР)		18	18
Защита контрольной работы			-
Защита курсовой работы			-
Защита курсового проекта			-
Промежуточная аттестация		2.35	2.35
Самостоятельная работа обучающихся (СРС)		78	78
в том числе:			
Курсовая работа			-
Курсовой проект			-
И / или другие виды самостоятельной работы: подготовка к лабораторным работам, практическим занятиям, контрольным работам, изучение теоретического материала		78	78
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. Управление информационной безопасностью на государственном уровне. Общие принципы и российская практика	Организационно-правовые формы управления безопасностью. Предпосылки развития государственного управления в сфере информационной безопасности. Общая методология и структура организационного обеспечения информационной безопасности на уровне государств. Общая политика России в сфере информационной безопасности. Структура органов государственной власти, обеспечивающих информационную безопасность в РФ.	1		
2	Раздел 2. Основные принципы построения SIEM	Средства визуализации элементов ИБ. Визуализация статистики по инцидентам ИБ. Комплексные системы мониторинга ИБ. Средства сбора отчетов и Logов. Основные принципы работы SIEM систем. Составление отчетов по ИБ.	1		
3	Раздел 3. Проведение комплекса процедур цифрового расследования в информационных и компьютерных системах	Digital Forensic. Расследование инцидентов. Утилиты для расследования инцидентов. Информация об истории посещения сайтов, кукисах, букмарках, скачанных файлах, заполненных формах, сохраненных логинах и т.д.	1		

4	Раздел 4. Введение в оценку и аудит ИБ путем выявления угроз ИБ «на лету»	Введение в «этический хакинг». Основные принципы его организации. Составление плана проведения тестирования целевой системы (инфраструктуры). Отношение к законодательству и регуляторам. Составление отчета и рекомендаций на основе проведенного тестирования.	1		
5	Раздел 5. Аудит систем удаленного и локального доступа	Основные механизмы и принципы проведения аудита ИБ СКУД предприятия, а также систем удаленного доступа с использованием технологий виртуальных частных сетей	1		
6	Раздел 6. Аудит инфраструктуры ИБ, интегрированных сервисов телефонии и беспроводного доступа	Основные механизмы и принципы проведения аудита ИБ инфраструктуры предприятия. Основные механизмы и принципы проведения аудита ИБ систем IP-телефонии, а также систем беспроводного доступа Wi-Fi	1		
7	Раздел 7. Принципы организации аудита систем информационной безопасности	Основные техники проведения аудита систем ИБ. Разработка методики проведения аудита систем ИБ. Основные средства проведения аудита систем ИБ.	1		
8	Раздел 8. Принципы построения интегрированных систем информационной безопасности	Создание политик ИБ предприятия. Принципы обеспечения безопасности инфраструктуры. Принципы обеспечения безопасности периметра сети телекоммуникационной системы. Регулирование правил работы СКУД. Регулирование правил удаленного доступа средствами VPN. Контроль безопасности конечных устройств. Контроль безопасности IP-телефонии.	1		
9	Раздел 9. Стандарты управления информационной безопасностью	Государственные стандарты в области ИБ РФ. Оценочные стандарты в информационной безопасности. Оранжевая книга. Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем. Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799. Их основные положения Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования"	1		
10	Раздел 10. Оценка рисков информационной безопасности	Основные составляющие информационной безопасности. Угрозы информационной безопасности в информационных системах. Основные определения и критерии, угрозы целостности и конфиденциальности.	1		

5.2. Междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами.

Таблица 5

№ п/п	Наименование обеспечиваемых (последующих) дисциплин

1	Вредоносное программное обеспечение

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. Управление информационной безопасностью на государственном уровне. Общие принципы и российская практика	4	2			8	14
2	Раздел 2. Основные принципы построения SIEM	2	2	2		8	14
3	Раздел 3. Проведение комплекса процедур цифрового расследования в информационных и компьютерных системах	2	2	2		8	14
4	Раздел 4. Введение в оценку и аудит ИБ путем выявления угроз ИБ «на лету»	2	2	2		8	14
5	Раздел 5. Аудит систем удаленного и локального доступа	2	4	2		8	16
6	Раздел 6. Аудит инфраструктуры ИБ, интегрированных сервисов телефонии и беспроводного доступа	2	2	2		8	14
7	Раздел 7. Принципы организации аудита систем информационной безопасности	2	2	2		8	14
8	Раздел 8. Принципы построения интегрированных систем информационной безопасности	4	2	2		8	16
9	Раздел 9. Стандарты управления информационной безопасностью	4	2	2		8	16
10	Раздел 10. Оценка рисков информационной безопасности	2	2	2		6	12
	Итого:	26	22	18	-	78	144

6. Лекции

Очная форма обучения

Таблица 7

№ п/п	Номер раздела	Тема лекции	Всего часов
1	1	Организационно-правовые формы управления безопасностью.	2
2	1	Общая методология и структура организационного обеспечения информационной безопасности на уровне государств.	2
3	2	Основные принципы работы SIEM систем.	2

4	3	Расследование инцидентов.	2
5	4	Введение в «этический хакинг».	2
6	5	Основные механизмы и принципы проведения аудита ИБ СКУД предприятия	2
7	6	Аудита ИБ инфраструктуры предприятия.	2
8	7	Основные техники проведения аудита систем ИБ.	2
9	8	Создание политик ИБ предприятия.	2
10	8	Контроль безопасности конечных устройств. Контроль безопасности IP-телефонии.	2
11	9	Международный стандарт ISO/IEC 15408.	2
12	9	Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799.	2
13	10	Угрозы информационной безопасности в информационных системах	2
		Итого:	26

7. Лабораторный практикум

Очная форма обучения

Таблица 8

№ п/п	Номер раздела	Наименование лабораторной работы	Всего часов
1	2	Исследование адресного пространства сети с использованием программ для аудита систем ИБ	2
2	3	Исследование последствий несанкционированного доступа к серверу под управлением ОС Windows	2
3	4	Оценка рисков ИБ предполагаемой компании в контексте угрозы землетрясений	2
4	5	Подбор оптимальных стандартов для разработки системы ИБ государственной компании	2
5	6	Проведение аудита VPN, построенной средствами IPsec, сети средствами ОС Kali Linux	2
6	7	Проведение аудита инфраструктуры IP-телефонии сети средствами ОС Kali Linux	2
7	8	Проведение аудита инфраструктуры беспроводного доступа к сети средствами ОС Kali Linux	2
8	9	Проведение аудита инфраструктуры сети средствами ОС Kali Linux	2
9	10	Разработка архитектуры интегрированной системы безопасности для организации концепции BYOD	2
		Итого:	18

8. Практические занятия (семинары)

Очная форма обучения

Таблица 9

№ п/п	Номер раздела	Тема занятия	Всего часов
1	1	Работа со стандартами ISO	2
2	2	Разработка доклада в компетентные органы на предмет нарушений в области ИБ	2
3	3	Разработка плана проведения атаки методом социальной инженерии для получения несанкционированного доступа к серверам	2

4	4	Разработка плана проведения аудита VPN, построенной средствами IPsec, сети средствами ОС Kali Linux	2
5	5	Разработка плана проведения аудита инфраструктуры IP-телефонии сети средствами ОС Kali Linux	2
6	5	Разработка плана проведения аудита инфраструктуры беспроводного доступа к сети средствами ОС Kali Linux	2
7	6	Разработка плана проведения аудита инфраструктуры сети средствами ОС Kali Linux	2
8	7	Разработка плана проведения исследование адресного пространства сети с использованием программ для аудита систем ИБ	2
9	8	Разработка плана проведения реализации концепции ИБ для гос. организации.	2
10	9	Разработка плана установления и развертывание opensource SIEM системы	2
11	10	Составление модели нарушите ИБ	2
		Итого:	22

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	Digital Forensic. Расследование инцидентов. Утилиты для расследования инцидентов. Подготовка к лабораторной работе.	отчёт	8
2	2	Введение в «этический хакинг». Подготовка к лабораторной работе.	отчёт	8
3	3	Государственные стандарты в области ИБ РФ. Подготовка к лабораторной работе.	отчёт	8
4	4	Организационно-правовые формы управления безопасностью. Подготовка к лабораторной работе.	отчёт	8
5	5	Основные механизмы и принципы проведения аудита ИБ инфраструктуры предприятия. Подготовка к лабораторной работе. Основные механизмы и принципы проведения аудита ИБ систем IP-телефонии, а также систем беспроводного доступа Wi-Fi	отчёт	8
6	6	Основные механизмы и принципы проведения аудита ИБ СКУД предприятия, а также систем удаленного доступа с использованием технологий виртуальных частных сетей. Подготовка к лабораторной работе.	отчёт	8
7	7	Основные составляющие информационной безопасности. Подготовка к лабораторной работе.	отчёт	8

8	8	Основные техники проведения аудита систем ИБ. Подготовка к лабораторной работе.	отчёт	8
9	9	Создание политик ИБ предприятия. Подготовка к лабораторной работе.	отчёт	8
10	10	Средства визуализации элементов ИБ. Подготовка к лабораторной работе.	отчёт	6
			Итого:	78

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 освоений дисциплины

12.1. Основная литература:

1. Андрианов, В. И.
   Инновационное управление рисками информационной безопасности : [Электронный ресурс] : учеб. пособие / В. И. Андрианов, А. В. Красов, В. А. Липатников ; рец.: С. Е. Душин, Е. В. Стельмашонок ; Федер. агентство связи, Федер. гос. образовательное бюдж. учреждение высш. проф. образования "С.-Петерб. гос. ун-т телекоммуникаций им. проф. М. А. Бонч-Бруевича". - СПб. : СПбГУТ, 2012. - 396 с. : ил. - Библиогр.: с. 394-395. - ISBN 978-5-91891-092-4 (в обл.) : 320.00 р.
2. Милославская, Н. Г.
   Управление рисками информационной безопасности. Учебное пособие для вузов : [Электронный ресурс] / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - М. : Горячая линия-Телеком, 2013. - 130 с. : ил. - URL: http://ibooks.ru/reading.php?productid=334011. - ISBN 978-5-9912-0272-5 : Б. ц.

3. Управление качеством систем менеджмента информационной безопасности : [Электронный ресурс] : учебное пособие / А. В. Красов [и др.] ; рец.: С. Е. Душин, Л. Б. Бузюков ; Федеральное агентство связи, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича". - СПб. : СПбГУТ, 2016. - 74 с. : ил. - 384.52 р.

4. Нормативное обеспечение эксплуатации средств защиты информации : [Электронный ресурс] : учебное пособие / А. В. Красов [и др.] ; рец.: А. А. Молдовян, Л. Б. Бузюков ; Федеральное агентство связи, Федеральное государственное бюджетное образовательное учреждение высшего образования "Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича". - СПб. : СПбГУТ, 2017. - 67 с. : ил. - 325.20 р.

12.2. Дополнительная литература:

1. Основы управления информационной безопасностью. Учебное пособие для вузов : [Электронный ресурс] / А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов и др. - М. : Горячая линия-Телеком, 2013. - 244 с. : ил. - URL: http://ibooks.ru/reading.php?productid=334010. - ISBN 978-5-9912-0271-8 : Б. ц.
2. Милославская, Н. Г.
   Проверка и оценка деятельности по управлению информационной безопасностью. Учебное пособие для вузов : [Электронный ресурс] / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - М. : Горячая линия-Телеком, 2013. - 166 с. : ил. - URL: http://ibooks.ru/reading.php?productid=334014. - ISBN 978-5-9912-0275-6 : Б. ц.

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:

- Linux
- 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 «Управление информационной безопасностью» 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
«Управление информационной безопасностью»

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. 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