**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 Информационных управляющих систем
(полное наименование кафедры)

Регистрационный № 24.02/272-Д

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Безопасность информационных технологий и систем
(наименование дисциплины)

образовательная программа высшего образования

09.03.02 Информационные системы и технологии
(код и наименование направления подготовки / специальности)

бакалавр
(квалификация)

Интеллектуальные информационные системы и технологии
(направленность / профиль образовательной программы)

очная форма, очно-заочная форма, заочная форма
(форма обучения)

Санкт-Петербург

Рабочая программа дисциплины составлена на основе требований Федерального государственного образовательного стандарта высшего образования по направлению (специальности) подготовки «09.03.02 Информационные системы и технологии», утвержденного приказом Министерства образования и науки Российской Федерации от 19.09.2017 № 926, и в соответствии с рабочим учебным планом, утвержденным ректором университета.

1. Цели и задачи дисциплины

Целью преподавания дисциплины «Безопасность информационных технологий и систем» является:

изучение теоретических и практических основ обеспечения информационной безопасности закрытых и открытых контуров компьютерных систем инфокоммуникационных инфраструктур. В результате изучения дисциплины у студентов должны сформироваться знания, умения и практические навыки, позволяющие разрабатывать политику информационной безопасности объектов защиты и организационно-практические меры по его защите.

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

получение студентами теоретических и прикладных знаний о современных методах обеспечения информационной безопасности закрытых и открытых контуров инфокоммуникационных систем.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Безопасность информационных технологий и систем» Б1.В.19 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки бакалавриата по направлению «09.03.02 Информационные системы и технологии». Изучение дисциплины «Безопасность информационных технологий и систем» опирается на знании дисциплин(ы) «Алгоритмы и структуры данных»; «Информационные системы разработки устройств телекоммуникаций»; «Основы теории сложных 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	ПК-33	Способен оценивать и следить за выполнением концептуально-логического проектирования систем и сопровождением разработанных проектных решений
2	УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

Индикаторы достижения компетенций

Таблица 2

ПК-33.1	Знать: методы концептуального-логического проектирования систем
ПК-33.2	Уметь: оценивать и следить за выполнением концептуального-логического проектирования систем и сопровождением разработанных проектных решений
ПК-33.3	Иметь навыки: концептуального-логического проектирования систем и сопровождения разработанных проектных решений

УК-2.1	Знать: виды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность.
УК-2.2	Уметь: проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; анализировать альтернативные варианты для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности.
УК-2.3	Владеть: методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта; навыками работы с нормативно-правовой документацией.

4. Объем дисциплины и виды учебной работы

Очная форма обучения

Таблица 3

Вид учебной работы		**Всего часов**	**Семестры**
			4
Общая трудоемкость	4 ЗЕТ	144	144
Контактная работа с обучающимися		52.35	52.35
в том числе:			
Лекции		20	20
Практические занятия (ПЗ)		16	16
Лабораторные работы (ЛР)		14	14
Защита контрольной работы			-
Защита курсовой работы			-
Защита курсового проекта			-
Промежуточная аттестация		2.35	2.35
Самостоятельная работа обучающихся (СРС)		58	58
в том числе:			
Курсовая работа			-
Курсовой проект			-
И / или другие виды самостоятельной работы: подготовка к лабораторным работам, практическим занятиям, контрольным работам, изучение теоретического материала		58	58
Подготовка к промежуточной аттестации		33.65	33.65
Вид промежуточной аттестации			Экзамен

Очно-заочная форма обучения

Таблица 4

Вид учебной работы		**Всего часов**	**Семестры**
			7
Общая трудоемкость	4 ЗЕТ	144	144
Контактная работа с обучающимися		36.35	36.35
в том числе:			
Лекции		14	14
Практические занятия (ПЗ)		12	12
Лабораторные работы (ЛР)		8	8
Защита контрольной работы			-
Защита курсовой работы			-

Защита курсового проекта		-
Промежуточная аттестация	2.35	2.35
Самостоятельная работа обучающихся (СРС)	71.65	71.65
в том числе:		
Курсовая работа		-
Курсовой проект		-
И / или другие виды самостоятельной работы: подготовка к лабораторным работам, практическим занятиям, контрольным работам, изучение теоретического материала	71.65	71.65
Подготовка к промежуточной аттестации	36	36
Вид промежуточной аттестации		Экзамен

Заочная форма обучения

Таблица 5

Вид учебной работы		**Всего часов**	**Семестры**		
			ус3	3	4
Общая трудоемкость	4 ЗЕТ	144	6	70	68
Контактная работа с обучающимися		12.65	6	4.3	2.35
в том числе:					
Лекции		4	4	-	-
Практические занятия (ПЗ)		4	-	4	-
Лабораторные работы (ЛР)		2	2	-	-
Защита контрольной работы		0.3	-	0.3	-
Защита курсовой работы			-	-	-
Защита курсового проекта			-	-	-
Промежуточная аттестация		2.35	-	-	2.35
Самостоятельная работа обучающихся (СРС)		122.35	-	65.7	56.65
в том числе:					
Курсовая работа			-	-	-
Курсовой проект			-	-	-
И / или другие виды самостоятельной работы: подготовка к лабораторным работам, практическим занятиям, контрольным работам, изучение теоретического материала		122.35	-	65.7	56.65
Подготовка к промежуточной аттестации		9	-	-	9
Вид промежуточной аттестации			-	-	Экзамен

5. Содержание дисциплины

5.1. Содержание разделов дисциплины.

Таблица 6

№ п/п	**Наименование раздела дисциплины**	**Содержание раздела**	**№ семестра**		
			очная	**очно-заоч-ная**	**заоч-ная**

1	Раздел 1. Информационная система как объект защиты	Тема 1.1. Эволюция архитектур информационных систем. Тема 1.2. Политика информационной безопасности объекта защиты. Описание объекта защиты. Определение основных приоритетов информационной безопасности. Тема 1.3. Анализ рисков. Формирование перечня критичных ресурсов. Модели нарушителя и угроз	4	7	3
2	Раздел 2. Требования информационной безопасности в закрытых и открытых контурах локальной вычислительной сети инфокоммуникационных систем	Тема 2.1. Общие требования построения защищенной информационной системы. Требования к подсистеме обеспечения безопасности сетевого взаимодействия. Тема 2.2. Требования к подсистеме аутентификации и управления доступом. Тема 2.3. Требования к подсистемам криптографической защиты информации и антивирусной защиты. Тема 2.4. Требования к подсистемам резервирования/восстановления информации, контроля эталонного состояния информации и рабочей среды. Тема 2.5. Требования к средствам построения защищенных виртуальных сетей (VPN) и управления безопасностью.	4	7	3
3	Раздел 3. Организационно-технические меры по реализации основных требований и построению системы информационной безопасности	Тема 3.1. Многоуровневая модель защиты в информационной системе на архитектуре «клиент-сервер»:методы защиты информации на физическом, канальном, сетевом, транспортном, сеансовом и прикладном уровнях модели ВОС.Протокол формирования защищенного туннеля на канальном уровне PPTP (Point-to-PointTunnelingProtocol). Протокол формирования защищенного туннеля на канальном уровне L2F (Layer-2 Forwarding). Протокол формирования защищенного туннеля на канальном уровне L2TP (Layer-2 TunnelingProtocol). Общее описание стека протоколов защиты межсетевого уровня IPsec (InternetProtocolSecurity). Протокол обмена ключевой информацией IKE (InternetKeyExchange). Протокол аутентифицирующего заголовка (AuthenticationHeader, AH). Протокол инкапсулирующей защиты содержимого (EncapsulatingSecurityPayload, ESP). Тема 3.2. Технические решения по защите межсетевого взаимодействия и передачи информации. Средства криптографической защиты информации. Тема 3.3. Технические решения по защите от вредоносного кода. Тема 3.4. Технические решения по защите от НСД компьютерных ресурсов на уровне серверов и рабочих станций ЛВС и реализации подсистемы аутентификации и идентификации	4	7	3

5.2. Междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами.

Таблица 7

№ п/п	Наименование обеспечиваемых (последующих) дисциплин
1	Архитектура информационных систем
2	Методы и средства проектирования информационных систем и технологий
3	Проектная оценка надежности информационных систем

5.3. Разделы дисциплин и виды занятий.

Очная форма обучения

Таблица 8

№ п/п	Наименование раздела дисциплины	Лекции	Практ. занятия	Лаб. занятия	Семинары	СРС	Всего часов
1	Раздел 1. Информационная система как объект защиты	2	4	4		18	28
2	Раздел 2. Требования информационной безопасности в закрытых и открытых контурах локальной вычислительной сети инфокоммуникационных систем	10	4	4		20	38
3	Раздел 3. Организационно-технические меры по реализации основных требований и построению системы информационной безопасности	8	8	6		20	42
	Итого:	20	16	14	-	58	108

Очно-заочная форма обучения

Таблица 9

№ п/п	Наименование раздела дисциплины	Лекции	Практ. занятия	Лаб. занятия	Семинары	СРС	Всего часов
1	Раздел 1. Информационная система как объект защиты	2	2	4		20	28
2	Раздел 2. Требования информационной безопасности в закрытых и открытых контурах локальной вычислительной сети инфокоммуникационных систем	6	2	2		20.65	30.65
3	Раздел 3. Организационно-технические меры по реализации основных требований и построению системы информационной безопасности	6	8	2		31	47
	Итого:	14	12	8	-	71.65	105.65

Заочная форма обучения

Таблица 10

№ п/п	Наименование раздела дисциплины	Лекции	Практ. занятия	Лаб. занятия	Семинары	СРС	Всего часов
1	Раздел 1. Информационная система как объект защиты	2				32.7	34.7
2	Раздел 2. Требования информационной безопасности в закрытых и открытых контурах локальной вычислительной сети инфокоммуникационных систем		2			33	35

3	Раздел 3. Организационно-технические меры по реализации основных требований и построению системы информационной безопасности	2	2	2		56.65	62.65
	Итого:	4	4	2	-	122.35	132.35

6. Лекции

Очная форма обучения

Таблица 11

№ п/п	Номер раздела	Тема лекции	Всего часов
1	1	Информационная система как объект защиты. Тема 1.1. Эволюция архитектур информационных систем. Тема 1.2. Политика информационной безопасности объекта защиты. Описание объекта защиты. Определение основных приоритетов информационной безопасности. Тема 1.3. Анализ рисков. Формирование перечня критичных ресурсов. Модели нарушителя и угроз	2
2	2	Тема 2.1. Требования информационной безопасности в закрытых и открытых контурах локальной вычислительной сети инфокоммуникационных систем Тема 2.1. Общие требования построения защищенной информационной системы. Требования к подсистеме обеспечения безопасности сетевого взаимодействия.	2
3	2	Тема 2.2. Требования к подсистеме аутентификации и управления доступом.	2
4	2	Тема 2.3. Требования к подсистемам криптографической защиты информации и антивирусной защиты.	2
5	2	Тема 2.4. Требования к подсистемам резервирования/восстановления информации, контроля эталонного состояния информации и рабочей среды.	2
6	2	Тема 2.5. Требования к средствам построения защищенных виртуальных сетей (VPN) и управления безопасностью.	2
7	3	Организационно-технические меры по реализации основных требований и построению системы информационной безопасности Тема 3.1. Многоуровневая модель защиты в информационной системе на архитектуре «клиент-сервер»:методы защиты информации на физическом, канальном, сетевом, транспортном, сеансовом и прикладном уровнях модели ВОС.Протокол формирования защищенного туннеля на канальном уровне PPTP (Point-to-PointTunnelingProtocol). Протокол формирования защищенного туннеля на канальном уровне L2F (Layer-2 Forwarding). Протокол формирования защищенного туннеля на канальном уровне L2TP (Layer-2 TunnelingProtocol). Общее описание стека протоколов защиты межсетевого уровня IPsec (InternetProtocolSecurity). Протокол обмена ключевой информацией IKE (InternetKeyExchange). Протокол аутентифицирующего заголовка (AuthenticationHeader, AH). Протокол инкапсулирующей защиты содержимого (EncapsulatingSecurityPayload, ESP).	2
8	3	Тема 3.2. Технические решения по защите межсетевого взаимодействия и передачи информации. Средства криптографической защиты информации.	2
9	3	Тема 3.3. Технические решения по защите от вредоносного кода.	2

10	3	Тема 3.4. Технические решения по защите от НСД компьютерных ресурсов на уровне серверов и рабочих станций ЛВС и реализации подсистемы аутентификации и идентификации.	2
		Итого:	20

Очно-заочная форма обучения

Таблица 12

№ п/п	Номер раздела	Тема лекции	Всего часов
1	1	Информационная система как объект защиты. Тема 1.1. Эволюция архитектур информационных систем. Тема 1.2. Политика информационной безопасности объекта защиты. Описание объекта защиты. Определение основных приоритетов информационной безопасности. Тема 1.3. Анализ рисков. Формирование перечня критичных ресурсов. Модели нарушителя и угроз	2
2	2	Тема 2.2. Требования к подсистеме аутентификации и управления доступом.	2
3	2	Тема 2.3. Требования к подсистемам криптографической защиты информации и антивирусной защиты.	2
4	2	Тема 2.4. Требования к подсистемам резервирования/восстановления информации, контроля эталонного состояния информации и рабочей среды.	2
5	3	Организационно-технические меры по реализации основных требований и построению системы информационной безопасности Тема 3.1. Многоуровневая модель защиты в информационной системе на архитектуре «клиент-сервер»:методы защиты информации на физическом, канальном, сетевом, транспортном, сеансовом и прикладном уровнях модели ВОС.Протокол формирования защищенного туннеля на канальном уровне PPTP (Point-to-PointTunnelingProtocol). Протокол формирования защищенного туннеля на канальном уровне L2F (Layer-2 Forwarding). Протокол формирования защищенного туннеля на канальном уровне L2TP (Layer-2 TunnelingProtocol). Общее описание стека протоколов защиты межсетевого уровня IPsec (InternetProtocolSecurity). Протокол обмена ключевой информацией IKE (InternetKeyExchange). Протокол аутентифицирующего заголовка (AuthenticationHeader, AH). Протокол инкапсулирующей защиты содержимого (EncapsulatingSecurityPayload, ESP).	4
6	3	Тема 3.2. Технические решения по защите межсетевого взаимодействия и передачи информации. Средства криптографической защиты информации.	2
		Итого:	14

Заочная форма обучения

Таблица 13

№ п/п	Номер раздела	Тема лекции	Всего часов
1	1	Информационная система как объект защиты. Тема 1.1. Эволюция архитектур информационных систем. Тема 1.2. Политика информационной безопасности объекта защиты. Описание объекта защиты. Определение основных приоритетов информационной безопасности. Тема 1.3. Анализ рисков. Формирование перечня критичных ресурсов. Модели нарушителя и угроз	2

2	3	Организационно-технические меры по реализации основных требований и построению системы информационной безопасности Тема 3.1. Многоуровневая модель защиты в информационной системе на архитектуре «клиент-сервер»:методы защиты информации на физическом, канальном, сетевом, транспортном, сеансовом и прикладном уровнях модели ВОС.Протокол формирования защищенного туннеля на канальном уровне PPTP (Point-to-PointTunnelingProtocol). Протокол формирования защищенного туннеля на канальном уровне L2F (Layer-2 Forwarding). Протокол формирования защищенного туннеля на канальном уровне L2TP (Layer-2 TunnelingProtocol). Общее описание стека протоколов защиты межсетевого уровня IPsec (InternetProtocolSecurity). Протокол обмена ключевой информацией IKE (InternetKeyExchange). Протокол аутентифицирующего заголовка (AuthenticationHeader, AH). Протокол инкапсулирующей защиты содержимого (EncapsulatingSecurityPayload, ESP).	2
		Итого:	4

7. Лабораторный практикум

Очная форма обучения

Таблица 14

№ п/п	Номер раздела	Наименование лабораторной работы	Всего часов
1	1	Информационная система как объект защиты	4
2	2	Требования информационной безопасности в закрытых и открытых контурах локальной вычислительной сети инфокоммуникационных систем	4
3	3	Организационно-технические меры по реализации основных требований и построению системы информационной безопасности	6
		Итого:	14

Очно-заочная форма обучения

Таблица 15

№ п/п	Номер раздела	Наименование лабораторной работы	Всего часов
1	1	Информационная система как объект защиты	4
2	2	Требования информационной безопасности в закрытых и открытых контурах локальной вычислительной сети инфокоммуникационных систем	2
3	3	Организационно-технические меры по реализации основных требований и построению системы информационной безопасности	2
		Итого:	8

Заочная форма обучения

Таблица 16

№ п/п	Номер раздела	Наименование лабораторной работы	Всего часов

1	3	Информационная система как объект защиты. Требования информационной безопасности в закрытых и открытых контурах локальной вычислительной сети инфокоммуникационных систем. Организационно-технические меры по реализации основных требований и построению системы информационной безопасности	2
		Итого:	2

8. Практические занятия (семинары)

Очная форма обучения

Таблица 17

№ п/п	Номер раздела	Тема занятия	Всего часов
1	1	Информационная система как объект защиты	4
2	2	Требования информационной безопасности в закрытых и открытых контурах локальной вычислительной сети инфокоммуникационных систем	4
3	3	Организационно-технические меры по реализации основных требований и построению системы информационной безопасности	4
4	3	Организационно-технические меры по реализации основных требований и построению системы информационной безопасности	4
		Итого:	16

Очно-заочная форма обучения

Таблица 18

№ п/п	Номер раздела	Тема занятия	Всего часов
1	1	Информационная система как объект защиты	2
2	2	Требования информационной безопасности в закрытых и открытых контурах локальной вычислительной сети инфокоммуникационных систем	2
3	3	Организационно-технические меры по реализации основных требований и построению системы информационной безопасности	2
4	3	Организационно-технические меры по реализации основных требований и построению системы информационной безопасности	6
		Итого:	12

Заочная форма обучения

Таблица 19

№ п/п	Номер раздела	Тема занятия	Всего часов
1	2	Требования информационной безопасности в закрытых и открытых контурах локальной вычислительной сети инфокоммуникационных систем	2
2	3	Организационно-технические меры по реализации основных требований и построению системы информационной безопасности	2
		Итого:	4

9. Примерная тематика курсовых проектов (работ)

Рабочим учебным планом не предусмотрено

10. Самостоятельная работа

Очная форма обучения

Таблица 20

№ п/п	Номер раздела	Содержание самостоятельной работы	Форма контроля	Всего часов
1	1	Информационная система как объект защиты	Собеседование	18
2	2	Требования информационной безопасности в закрытых и открытых контурах локальной вычислительной сети инфокоммуникационных систем	Собеседование	20
3	3	Организационно-технические меры по реализации основных требований и построению системы информационной безопасности	Собеседование	20
			Итого:	58

Очно-заочная форма обучения

Таблица 21

№ п/п	Номер раздела	Содержание самостоятельной работы	Форма контроля	Всего часов
1	1	Информационная система как объект защиты	Собеседование	20
2	2	Требования информационной безопасности в закрытых и открытых контурах локальной вычислительной сети инфокоммуникационных систем	Собеседование	20.65
3	3	Организационно-технические меры по реализации основных требований и построению системы информационной безопасности	Собеседование	31
			Итого:	71.65

Заочная форма обучения

Таблица 22

№ п/п	Номер раздела	Содержание самостоятельной работы	Форма контроля	Всего часов
1	1	Информационная система как объект защиты	Собеседование	32.7
2	2	Требования информационной безопасности в закрытых и открытых контурах локальной вычислительной сети инфокоммуникационных систем	Собеседование	33
3	3	Организационно-технические меры по реализации основных требований и построению системы информационной безопасности	Собеседование	56.65
			Итого:	122.35

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

13.1. Основная литература:

1. Мельников, Д. А.
   Информационная безопасность открытых систем : [Электронный ресурс] / Д.А. Мельников. - М. : Флинта, 2019. - 448 с. : ил. - URL: http://ibooks.ru/reading.php?productid=340843. - ISBN 978-5-9765-1613-7 : Б. ц.
2. Шаньгин, В. Ф.
   Информационная безопасность компьютерных систем и сетей : [Электронный ресурс] : учебное пособие / Шаньгин В. Ф. - М. : ФОРУМ ; М. : ИНФРА-М, 2021. - 416 с. - URL: http://ibooks.ru/reading.php?productid=361273. - ISBN 978-5-8199-0754-2 : Б. ц.

13.2. Дополнительная литература:

1. Защита информации и информационная безопасность. Эффективность комплексных систем защиты информации в телекоммуникациях : учебное пособие / Л. К. Птицына, Л. Г. Осовецкий, А. В. Птицын, М. В. Солнцев. - СПб. : Изд-во Политехн. ун-та, 2007. - 107 с. : ил. - ISBN 5-7422-1402-2 : 175.00 р. - Текст : непосредственный.
2. Птицын, А. В.
Генерация системно-аналитического ядра безопасных информационных технологий / А. В. Птицын, Л. К. Птицына ; рец. В. Н. Громов. - СПб. : Изд-во Политехн. ун-та, 2011. - 262, [1] с. : ил. - Библиогр.: с. 243-262. - ISBN 978-5-7422-3143-1 (в обл.) : 415.00 р. - Текст : непосредственный.

3. Нормативное обеспечение эксплуатации средств защиты информации : [Электронный ресурс] : учеб. пособие / А. В. Красов, И. И. Лившиц, Д. В. Юркин [и др.] ; рец.: А. А. Молдовян, Л. Б. Бузюков ; Федер. агентство связи, Федер. гос. бюдж. образовательное учреждение высш. образования "С.-Петерб. гос. ун-т телекоммуникаций им. проф. М. А. Бонч-Бруевича". - СПб. : СПбГУТ, 2017. - 67 с. : ил. - 325.20 р.

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:

- Open Office
- Google Chrome

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 «Безопасность информационных технологий и систем» 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 23

№ 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
«Безопасность информационных технологий и систем»

Код и наименование направления подготовки/специальности:
09.03.02 Информационные системы и технологии
Направленность/профиль образовательной программы:
Интеллектуальные информационные системы и технологии

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