Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Исаев Игорь Магомедович
Должность: Проректор по безопасности и общим вопросам
Дата подписания: 28.04.2023 10:06:27
Уникальный программный ключ:
d7a26b9e8ca85e98ec3de2eb454b4659d961f249

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский технологический университет «МИСиС»

Рабочая программа дисциплины (модуля)

Защита информации

Закреплена за подразделением Кафедра АСУ

Направление подготовки 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

Профиль

Квалификация **Бакалавр**
Форма обучения **очная**
Общая трудоемкость **4 ЗЕТ**

Часов по учебному плану 144
в том числе:
аудиторные занятия 48
самостоятельная работа 69
часов на контроль 27

Формы контроля в семестрах:
экзамен 8

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**8 (4.2)**		Итого	
Недель	12			
Вид занятий	УП	РП	УП	РП
Лекции	24	24	24	24
Лабораторные	24	24	24	24
Итого ауд.	48	48	48	48
Контактная работа	48	48	48	48
Сам. работа	69	69	69	69
Часы на контроль	27	27	27	27
Итого	144	144	144	144

Программу составил(и):
асс., Нгуен Туан Минь

Рабочая программа
Защита информации

Разработана в соответствии с ОС ВО:

Самостоятельно устанавливаемый образовательный стандарт высшего образования - бакалавриат Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский технологический университет «МИСиС» по направлению подготовки 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА (приказ от 02.04.2021 г. № 119 о.в.)

Составлена на основании учебного плана:

09.03.01 Информатика и вычислительная техника, 09.03.01-БИВТ-22.plx , утвержденного Ученым советом ФГАОУ ВО НИТУ "МИСиС" в составе соответствующей ОПОП ВО 22.09.2022, протокол № 8-22

Утверждена в составе ОПОП ВО:

09.03.01 Информатика и вычислительная техника, , утвержденной Ученым советом ФГАОУ ВО НИТУ "МИСиС" 22.09.2022, протокол № 8-22

Рабочая программа одобрена на заседании
Кафедра АСУ

Протокол от 05.07.2022 г., №10

Руководитель подразделения Темкин Игорь Олегович, д.т.н., доцент

1. ЦЕЛИ ОСВОЕНИЯ	
1.1	- Понимание основных определений и характеристик информационной безопасности;
1.2	- Описание общих операционных системы и освоение принципов пересылки брандмауэров;
1.3	- Обеспечение базовых настроек и обслуживание решений информационной безопасности для малых и средних предприятий.

2. МЕСТО В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Блок ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	MES-системы
2.1.2	Искусственный интеллект в прикладных задачах управления
2.1.3	Методология построения интеллектуальных платформ
2.1.4	Методы поиска решений
2.1.5	Модели управления автономными транспортными комплексами
2.1.6	Научно-исследовательская работа
2.1.7	Научно-исследовательская работа
2.1.8	Научно-исследовательская работа
2.1.9	Научно-исследовательская работа
2.1.10	Облачные технологии и распределенные базы данных
2.1.11	Оптимизационное моделирование сложных систем
2.1.12	Основы разработки цифровых платформ управления
2.1.13	Программирование встраиваемых систем
2.1.14	Программные инструменты BI-систем
2.1.15	Проектирование и разработка программных комплексов Ч.2
2.1.16	Проектирование интеллектуальных систем управления
2.1.17	Проектирование систем управления взаимодействием распределенных объектов
2.1.18	Управление проектами
2.1.19	UX/UI - дизайн
2.1.20	Автоматизация технологических процессов
2.1.21	Введение в обработку больших данных
2.1.22	Интеллектуальный анализ данных
2.1.23	Математические модели социально-экономических систем
2.1.24	Методология разработки программного обеспечения
2.1.25	Методы оптимизации
2.1.26	Мультиагентное моделирование систем
2.1.27	Нейросетевые технологии в управлении
2.1.28	Проектирование и разработка программных комплексов Ч.1
2.1.29	Производственная практика
2.1.30	Производственная практика
2.1.31	Производственная практика
2.1.32	Производственная практика
2.1.33	Системы реального времени
2.1.34	Технологии решения задач машинного обучения
2.1.35	Введение в прикладной ИИ
2.1.36	Учебная практика
2.1.37	Учебная практика
2.1.38	Учебная практика
2.1.39	Учебная практика
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**

3. РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ФОРМИРУЕМЫМИ КОМПЕТЕНЦИЯМИ

ПК-5: Способность и готовность применять современные языки программирования, операционные системы, современные инструменты хранения, обработки и анализа данных, способы и механизмы управления данными, программировать приложения и создавать программные прототипы решения прикладных задач
Знать:
ПК-5-З1 Основные понятия информационной безопасности, ее стандарты и спецификации. Основные концепции сети и работа с сетевыми устройствами. Понятие операционной системы и цели ее работы.
ПК-2: Способность использовать стандартные библиотеки прикладных программ и приложения для решения практических задач, отлаживать и тестировать компоненты программного обеспечения
Знать:
ПК-2-З1 Принципы построения и функционирования сетей и протоколов стека TCP/IP; модели ISO/OSI; Понимание принципов компьютерной и сетевой безопасности, безопасности web-приложений; Знание принципов работы средств обеспечения безопасности.
ОПК-7: Способен участвовать в настройке и наладке программно-аппаратных комплексов
Знать:
ОПК-7-З1 Механизм шифрования и дешифрования; Криптографические технологий: инфраструктуру открытых ключей (PKI) и систему сертификатов; Методы оценки безопасности и ключевые моменты анализа журналов; Процессы и принципы цифровой криминалистики.
ПК-5: Способность и готовность применять современные языки программирования, операционные системы, современные инструменты хранения, обработки и анализа данных, способы и механизмы управления данными, программировать приложения и создавать программные прототипы решения прикладных задач
Уметь:
ПК-5-У1 Работать с сетевыми устройствами, операционными системами на уровне администратора; Настраивать сервисы такие, как DNS, DHCP.
ПК-2: Способность использовать стандартные библиотеки прикладных программ и приложения для решения практических задач, отлаживать и тестировать компоненты программного обеспечения
Уметь:
ПК-2-У1 Настраивать протоколы, сценарии и внедрять технологию AAA на межсетевом экране; Проводить операции по мониторингу и обеспечению безопасности.
ОПК-7: Способен участвовать в настройке и наладке программно-аппаратных комплексов
Уметь:
ОПК-7-У1 Разрабатывать технические и аналитические документации; Проводить статистические исследования; Расследовать инциденты безопасности, сбор доказательной базы, форензика;
ПК-5: Способность и готовность применять современные языки программирования, операционные системы, современные инструменты хранения, обработки и анализа данных, способы и механизмы управления данными, программировать приложения и создавать программные прототипы решения прикладных задач
Владеть:
ПК-5-В1 Навыками работы с VirtualBox и VMware Workstation, настройки и тестирования сети.
ПК-2: Способность использовать стандартные библиотеки прикладных программ и приложения для решения практических задач, отлаживать и тестировать компоненты программного обеспечения
Владеть:
ПК-2-В1 Навыками использования в инфраструктуре работодателя (прим.: Huawei) профильного ПО. Проведения операций по обеспечению безопасности.
ОПК-7: Способен участвовать в настройке и наладке программно-аппаратных комплексов
Владеть:
ОПК-7-В1 Навыками выявления угроз ИБ на основе сведений об уязвимостях (классификация угроз, формирование рекомендаций по устранению уязвимостей и минимизации бизнес-рисков);

4. СТРУКТУРА И СОДЕРЖАНИЕ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Формируемые индикаторы компетенций	Литература и эл. ресурсы	Примечание	КМ	Выполняемые работы

	Раздел 1. 1. Основные понятия информационной безопасности. Стандарты и спецификации. Основные концепции сети.							
1.1	Основные конфигурации сети. /Лаб/	8	2	ПК-5-У1 ПК-5-В1	Л1.2 Л1.3 Л1.1Л2.3 Л2.1 Э1			Р1
1.2	Изучение главы 101 из материалов HCIA-Security /Ср/	8	3	ПК-5-З1 ПК-5-У1 ПК-5-В1	Э2			
1.3	Изучение главы 102 из материалов HCIA-Security /Ср/	8	3	ПК-5-З1 ПК-5-У1 ПК-5-В1	Э2			
1.4	Изучение главы 103 из материалов HCIA-Security /Ср/	8	3	ПК-5-З1 ПК-5-У1 ПК-5-В1	Э2			
1.5	Основные понятия информационной безопасности. Стандарты и спецификации. Основные концепции сети. /Лек/	8	2	ПК-5-З1	Л1.1 Л1.2 Л1.3 Л1.1Л2.3 Л2.1			
	Раздел 2. 2. Общие сетевые устройства. Распространенные угрозы информационной безопасности. Тенденции развития защиты потоков и информационной безопасности.							
2.1	Политики безопасности межсетевого экрана (Firewall) /Лаб/	8	2	ПК-5-З1 ПК-5-У1	Л1.4 Л1.1 Л1.2 Л1.3 Л1.1Л2.3 Л2.1 Э1		КМ1	Р2
2.2	Изучение главы 105 из материалов HCIA-Security /Ср/	8	3	ПК-5-З1 ПК-5-У1 ПК-5-В1	Э2			
2.3	Изучение главы 104 из материалов HCIA-Security /Ср/	8	3	ПК-5-З1 ПК-5-У1 ПК-5-В1	Э2			
2.4	Изучение главы 106 из материалов HCIA-Security /Ср/	8	3	ПК-5-З1 ПК-5-У1 ПК-5-В1	Э2			
2.5	Общие сетевые устройства. Распространенные угрозы информационной безопасности. Тенденции развития защиты потоков и информационной безопасности. /Лек/	8	4	ПК-5-З1	Л1.1 Л1.2 Л1.3 Л1.1Л2.3 Л2.1			
	Раздел 3. 3. Обзор операционной системы. Распространенные типы серверов и угрозы. Хост-брандмауэр и антивирусное программное обеспечение. Введение в брандмауэры.							
3.1	NAT-сервер межсетевого экрана и исходный NAT. /Лаб/	8	4	ПК-5-З1 ПК-5-У1	Л1.2 Л1.3 Л1.1Л2.3 Л2.1 Э1			Р3

3.2	Изучение главы 107 из материалов HCIA-Security /Ср/	8	3	ПК-5-З1 ПК-5-У1 ПК-5-В1	Э2			
3.3	Изучение главы 108 из материалов HCIA-Security /Ср/	8	4	ПК-5-З1 ПК-5-У1 ПК-5-В1	Э2			
3.4	Изучение главы 109 из материалов HCIA-Security /Ср/	8	4	ПК-5-З1 ПК-5-У1 ПК-5-В1	Э2			
3.5	Изучение главы 110 из материалов HCIA-Security /Ср/	8	4	ПК-5-З1 ПК-5-У1 ПК-5-В1	Э2			
3.6	Обзор операционной системы. Распространенные типы серверов и угрозы. Хост-брандмауэр и антивирусное программное обеспечение. Введение в брандмауэры. /Лек/	8	4	ПК-5-З1	Л1.1 Л1.2 Л1.3 Л1.1Л2.3 Л2.1			
	Раздел 4. 4. Преобразование сетевых адресов (NAT). Горячее резервирование двойной системы (Dual-System Hot Standby). Управление пользователями брандмауэра.							
4.1	Горячий резерв межсетевого экрана (Hot Standby). /Лаб/	8	4	ПК-2-З1 ПК-2-У1	Л1.4 Л2.3 Л2.1 Л1.1 Л1.2 Л1.3 Л1.1 Э1		КМ2	Р4
4.2	Изучение главы 111 из материалов HCIA-Security /Ср/	8	3	ПК-2-З1 ПК-2-У1 ПК-2-В1	Э2			
4.3	Изучение главы 112 из материалов HCIA-Security /Ср/	8	3	ПК-2-З1 ПК-2-У1 ПК-2-В1	Э2			
4.4	Изучение главы 113 из материалов HCIA-Security /Ср/	8	3	ПК-2-З1 ПК-2-У1 ПК-2-В1	Э2			
4.5	Преобразование сетевых адресов (NAT). Горячее резервирование двойной системы (Dual-System Hot Standby). Управление пользователями брандмауэра. /Лек/	8	4	ПК-2-З1	Л1.1 Л1.2 Л1.3 Л1.1Л2.3 Л2.1			
	Раздел 5. 5. Обзор предотвращения вторжений. Механизм шифрования и дешифрования. Инфраструктура открытых ключей (PKI). Система сертификатов. Применение криптографических технологий.							
5.1	Управление пользователями межсетевого экрана. /Лаб/	8	4	ПК-2-З1 ПК-2-У1	Л1.4 Л2.1 Л1.1 Л1.2 Л1.1Л2.3 Э1			Р5

5.2	Изучение главы 114 из материалов HCIA-Security /Ср/	8	3	ПК-2-З1 ПК-2-У1 ПК-2-В1	Э2			
5.3	Изучение главы 115 из материалов HCIA-Security /Ср/	8	3	ПК-2-З1 ПК-2-У1 ПК-2-В1	Э2			
5.4	Изучение главы 116 из материалов HCIA-Security /Ср/	8	3	ПК-2-З1 ПК-2-У1 ПК-2-В1	Э2			
5.5	Обзор предотвращения вторжений. Механизм шифрования и дешифрования. Инфраструктура открытых ключей (PKI). Система сертификатов. Применение криптографических технологий. /Лек/	8	4	ПК-2-З1	Л1.1 Л1.2 Л1.3 Л1.1Л2.3 Л2.1			
	Раздел 6. 6. Введение в операции по обеспечению безопасности. Отслеживание и анализ данных.							
6.1	L2TP VPN. /Лаб/	8	4	ПК-2-З1 ПК-2-У1	Л1.4 Л2.1 Л1.1Л2.3 Э1			Р6
6.2	Изучение главы 118 из материалов HCIA-Security /Ср/	8	3	ПК-2-З1 ПК-2-У1 ПК-2-В1	Э2			
6.3	Изучение главы 119 из материалов HCIA-Security /Ср/	8	3	ПК-2-З1 ПК-2-У1 ПК-2-В1	Э2			
6.4	Введение в операции по обеспечению безопасности. Отслеживание и анализ данных. /Лек/	8	2	ПК-2-З1	Л1.1 Л1.2 Л1.3 Л1.1Л2.3 Л2.1			
	Раздел 7. 7. Цифровая криминалистика. Реагирования на чрезвычайные ситуации кибербезопасности.							
7.1	GRE VPN. /Лаб/	8	4	ОПК-7-З1 ОПК-7-У1	Л2.3 Л2.1 Л1.1Л1.4 Л1.1 Э1		КМ3	Р7
7.2	Изучение главы 120 из материалов HCIA-Security /Ср/	8	6	ОПК-7-З1 ОПК-7-У1 ОПК-7-В1	Э2			
7.3	Изучение главы 121 из материалов HCIA-Security /Ср/	8	6	ОПК-7-З1 ОПК-7-У1 ОПК-7-В1	Э2			
7.4	Цифровая криминалистика. Реагирования на чрезвычайные ситуации кибербезопасности. /Лек/	8	4	ОПК-7-З1	Л1.1 Л1.2 Л1.3 Л1.1Л2.3 Л2.1			

5. ФОНД ОЦЕНОЧНЫХ МАТЕРИАЛОВ

5.1. Контрольные мероприятия (контрольная работа, тест, коллоквиум, экзамен и т.п), вопросы для самостоятельной подготовки

Код КМ	Контрольное мероприятие	Проверяемые индикаторы компетенций	Вопросы для подготовки

КМ1	Контрольные вопросы №1	ПК-5-З1;ПК-5-У1;ПК-5-В1	- Методы атак на систему безопасности, влекущие за собой инциденты, связанные с нарушением информационной безопасности. Международные стандарты информационной безопасности; - Фазы модели системы ISMS(СМИБ); - Уровни модели TCP/IP. Процесс трехэтапного рукопожатия соединения TCP; - Базовые сетевые устройства. Понятие межсетевого экрана (Фаэрвол), коммутатора и маршрутизатора; - Функционал зон безопасности и какие зоны безопасности включает в себя межсетевой экран; - Угрозы безопасности приложений и риски безопасности устройств; - Ключевые элементы защиты информационной безопасности.
КМ2	Контрольные вопросы №2	ПК-2-З1;ПК-2-У1;ПК-2-В1	- Типы серверов. Угрозы безопасности, влияющие на работу сервера; - Понятие уязвимости, их причины и классификация; - Понятие межсетевого экрана(Фаэрвол), классификация, зоны безопасности; - Компоненты антивирусного приложения; - NAT: преимущества/недостатки, категории (базированные на сценариях применения); - Основные принципы протоколов VRRP/VGMP/HRP; - Технология AAA; - Классификация пользователей/режимы входа администратора.
КМ3	Контрольные вопросы №3	ОПК-7-З1;ОПК-7-У1;ОПК-7-В1	- Сетевые угрозы в современной сети; - Понятие вторжения. Система предотвращения вторжений (IPS); - Категории компьютерных вирусов и их взаимосвязь; - Алгоритмы криптографий. Функции и типы технологий шифрования; - Цифровые сертификаты (типы, структура, форматы и др.); - Базовые условия для мониторинга безопасности (Security operations). Условия проведения операций по обеспечению безопасности; - Методы оценки безопасности. Ключевые моменты анализа журналов; - Киберпреступление: характеристики/мотивы/формы; - Цифровая криминалистика, ее процесс и принципы. Цифровые улики; - Классификация инцидентов кибербезопасности; - Реагирования на чрезвычайные ситуации и их уровни; - Модель PDRR.

5.2. Перечень работ, выполняемых по дисциплине (Курсовая работа, Курсовой проект, РГР, Реферат, ЛР, ПР и т.п.)

Код работы	Название работы	Проверяемые индикаторы компетенций	Содержание работы
Р1	Лабораторная работа №1. Основные конфигурации сети.	ПК-5-У1;ПК-5-В1;ПК-2-В1	Настройка статических маршрутов (static routes), с целью изучения основных методов настройки сети.
Р2	Лабораторная работа №2. Политики безопасности межсетевого экрана (Firewall)	ПК-2-З1;ПК-2-У1;ПК-2-В1	Развертывание политики безопасности на межсетевом экране, с целью гарантии получения активного доступа к зоне недоверия (Untrust zone) из зоны доверия (Trust zone).
Р3	Лабораторная работа №3. NAT-сервер межсетевого экрана и исходный NAT.	ПК-2-З1;ПК-2-У1;ПК-2-В1	Настройка NAT. Получение доступа к Интернету, используя небольшое количество общедоступных IP-адресов, и получение доступа к серверу интрасети через определенные IP-адреса.

Р4	Лабораторная работа №4. Горячий резерв межсетевого экрана (Hot Standby).	ПК-2-В1;ПК-2-У1;ОПК-7-З1	Развертывание двух или более межсетевых экранов на выходе из сети для обеспечения связи между Интранетом и Интернетом.
Р5	Лабораторная работа №5. Управление пользователями межсетевого экрана.	ПК-2-В1;ОПК-7-З1	Развертывание устройства безопасности на выходе из сети: подход позволяет осуществлять локальную проверку подлинности или же наоборот освобождать ее от проверки пользователям, имеющим доступ в Интернет, тем самым реализуя их управление.
Р6	Лабораторная работа №6. L2TP VPN.	ПК-2-В1;ПК-2-У1;ОПК-7-У1	Установка ПО VPN Client на компьютер и настройка VPN-туннель L2TP между VPN Client и корпоративным выходным шлюзом LNS для доступа к интрасети через VPN-туннель.
Р7	Лабораторная работа №7. GRE VPN.	ПК-2-В1;ОПК-7-З1;ПК-2-У1	Установка туннеля GRE между двумя сетевыми экранами, чтобы частные IP-сети могли обмениваться информацией о статических маршрутах через Интернет.

5.3. Оценочные материалы, используемые для экзамена (описание билетов, тестов и т.п.)

Экзаменационный билет состоит из двух теоретических вопросов. Билеты хранятся на кафедре.

5.4. Методика оценки освоения дисциплины (модуля, практики. НИР)

По дисциплине предусмотрены:
- Отчеты по лабораторным работам, состоящие из условия задачи, хода работы и пояснительной части;
- Оценки за контрольные вопросы;
- Курсовая работа (тема обсуждается с лектором дисциплины).

За текущую учебную деятельность обучающегося при выполнении каждой лабораторной работы (выполнение, защита и предоставление отчета), а также ответов на контрольные вопросы, выставляются оценки по 5-балльной (государственной) шкале.
Итоговая оценка определяется на основе правильности, целостности и сдачи в срок выполненных обучающимся заданий.

Промежуточная аттестация в форме учета выполненного минимума (Лабораторные работы 1-4, КМ1, КМ2) позволяет оценить уровень сформированности компетенций в целом по дисциплине и может осуществляться, как в письменной так и в устной форме.

По окончании изучения дисциплины в системе оценки знаний и умений используются следующие критерии:
«Отлично» – за глубокое и полное овладение содержанием учебного материала, в котором студент легко ориентируется, владение понятийным аппаратом за умение связывать теорию с практикой, решать практические задачи, высказывать и обосновывать свои суждения. Отличная отметка предполагает грамотное, логичное изложение ответа (как в устной, так и в письменной форме), качественное внешнее оформление;
«Хорошо» – если студент полно освоил учебный материал, владеет понятийным аппаратом, ориентируется в изученном материале, осознанно применяет знания для решения практических задач, грамотно излагает ответ, но содержание и форма ответа имеют некоторые неточности;
«Удовлетворительно»– если студент обнаруживает знание и понимание основных положений учебного материала, но излагает его неполно, непоследовательно, допускает неточности в определение понятий, в применении знаний для решения практических задач, не умеет доказательно обосновать свои суждения;
«Неудовлетворительно» – если студент имеет разрозненные, бессистемные знания, не умеет выделять главное и второстепенное, допускает ошибки в определение понятий, искажает их смысл, беспорядочно и неуверенно излагает материал, не может применять знания для решения практических задач; за полное незнание и непонимание учебного материала или отказ отвечать.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Библиотека	Издательство, год
Л1.1	Рытенкова О.	Информационная безопасность: журнал	Электронная библиотека	Москва: ГРОТЕК, 2013
Л1.2	Гладких Т. В., Воронова Е. В.	Информационные системы и сети: учебное пособие	Электронная библиотека	Воронеж: Воронежский государственный университет инженерных технологий, 2016

	Авторы, составители	Заглавие	Библиотека	Издательство, год
Л1.3	Никифоров С. В.	Введение в сетевые технологии. Элементы применения и администрирования сетей: учеб. пособие для студ. вузов, обуч. по спец. 351400 "Прикладная информатика" и др. междисциплинарным спец.	Библиотека МИСиС	М.: Финансы и статистика, 2005

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Библиотека	Издательство, год
Л2.1		Безопасность и надежность технических систем: учебное пособие	Электронная библиотека	Москва: Логос, 2004
Л2.2	Крынецкая Г. С.	Сетевые технологии: практикум	Электронная библиотека	М.: Изд-во МИСиС, 2008

6.1.3. Методические разработки

	Авторы, составители	Заглавие	Библиотека	Издательство, год
Л3.1	Щербаков А.	Современная компьютерная безопасность. Теоретические основы. Практические аспекты: учебное пособие	Электронная библиотека	Москва: Книжный мир, 2009
Л3.2	Башлы П. Н., Баранова Е. К., Бабаш А. В.	Информационная безопасность: учебно-практическое пособие: учебное пособие	Электронная библиотека	Москва: Евразийский открытый институт, 2011

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Э1	HCIA Security	https://forum.huawei.com/enterprise/ru/hcia-security-%D1%83%D1%87%D0%B5%D0%B1%D0%BD%D1%8B%D0%B5-%D0%BC%D0%B0%D1%82%D0%B5%D1%80%D0%B8%D0%B0%D0%BB%D1%8B/thread/721971-100153
Э2	HCIA-Security V3.0 Course	https://talent.huaweiuniversity.com/portal/courses/HuaweiX+EBGTC00000312/about

6.3 Перечень программного обеспечения

6.4. Перечень информационных справочных систем и профессиональных баз данных

И.1	https://habr.com
И.2	https://forum.huawei.com/
И.3	https://www.tune-it.ru/

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ

Дисциплина требует значительного объема самостоятельной работы.
Отдельные учебные или же технические вопросы обсуждаются с преподавателем во время лабораторных занятий.
Качественно освоить дисциплину возможно только при систематической самостоятельной работе, что поддерживается системой текущей и рубежной аттестации. Работы выполняются на платформе eNSP, как для выполнения, так и для их оформления.
В процессе выполнения лабораторных работ необходимо показать умелое применение полученных в процессе обучения знаний и навыков таких, как: имитационное моделирование, основы теории информации, информационная безопасность, сетевые технологии, вычислительные машины, сети и системы.
При выполнении работ акцент делается на формирование навыков работы студентов с научно-технической литературой; работы с документацией HCIA-Security, eNSP; на систематизацию материала для решения поставленных задач; на формирование навыков оформления результатов выполненных работ. Индивидуальные задания на курсовую работу студент получает у преподавателя в соответствии с прилагаемым перечнем их тематик. Рекомендуемая форма их оформления – отчеты с приложением программного файла ЭИОР «Canvas». Защита работы проводится индивидуально каждым студентом. Студенты делают сообщение и отвечают на вопросы преподавателя.
При подготовке к экзамену необходимо опираться на вопросы выходного контроля знаний, основную и дополнительную литературу, другие источники информации.