МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

УТВЕРЖДАЮ:

Директор ИТТСУ

П.Ф. Бестемьянов

26 мая 2020 г.

Кафедра «Управление и защита информации»

Автор Клепцов Михаил Яковлевич, д.т.н., профессор

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Основы построения защищенных компьютерных сетей

Специальность:	10.05.01 – Компьютерная безопасность
Специализация:	Информационная безопасность объектов информатизации на базе компьютерных систем
Квалификация выпускника:	Специалист по защите информации
Форма обучения:	очная
Год начала подготовки	2020

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 10 26 мая 2020 г. Председатель учебно-методической комиссии  С.В. Володин	Протокол № 16 21 мая 2020 г. Заведующий кафедрой  Л.А. Баранов

Москва 2020 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью изучения дисциплины «Основы построение защищенных компьютерных сетей» является теоретическая и практическая подготовка обучающихся к деятельности, связанной с построением защищенных сетевых автоматизированных систем, а также обучение принципам и методам защиты информации в компьютерных сетях.
Задачи дисциплины:
- изучение типовых угроз безопасности в компьютерных сетях;
- изучение криптографических и программно-аппаратных методов обеспечения информационной безопасности в компьютерных сетях;
- приобретение навыков настройки и эксплуатации средств обеспечения безопасности в компьютерных сетях;
- овладение средствами и методами проектирования и построения защищенных сетевых автоматизированных систем;
- овладение средствами и методами выявления и нейтрализации попыток нарушения безопасности в компьютерных сетях.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Учебная дисциплина "Основы построения защищенных компьютерных сетей" относится к блоку 1 "Дисциплины (модули)" и входит в его базовую часть.

2.1. Наименования предшествующих дисциплин

Для изучения данной дисциплины необходимы следующие знания, умения и навыки, формируемые предшествующими дисциплинами:

2.1.1. Основы информационной безопасности :

Знания: основных средств и способов обеспечения информационной безопасности, принципов построения систем защиты информации

Умения: владение профессиональной терминологией в области информационной безопасности

Навыки: использование основных средств и способов обеспечения информационной безопасности, принципов построения систем защиты информации

2.1.2. Языки программирования:

Знания: языков программирования высокого уровня и языка ассемблера персонального компьютера

Умения: применять языки программирования высокого уровня и языки ассемблера персонального компьютера

Навыки: владение навыками разработки, документирования, тестирования и отладки программ

2.2. Наименование последующих дисциплин

Результаты освоения дисциплины используются при изучении последующих учебных дисциплин:

2.2.1. Объекты защиты информации

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

В результате освоения дисциплины студент должен:

№ п/п	Код и название компетенции	Ожидаемые результаты
1	ОПК-10 Способен администрировать подсистемы и средства защиты информации в компьютерных системах и сетях	ОПК-10.1 Выполняет задачи по администрированию подсистем и средств защиты информации в КС. ОПК-10.2 Выполняет задачи по администрированию подсистем и средств защиты информации в сетях.
2	ОПК-16 Способен оценивать эффективность реализации действующих политик безопасности операционных систем и систем управления базами данных	ОПК-16.1 Владеет методами и средствами оценки эффективности операционных систем и систем управления базами данных. ОПК-16.2 Умеет применять на практике методы и средства оценки эффективности операционных систем и систем управления базами данных. ОПК-16.3 Умеет проводить дифференциацию и декомпозицию задач оценки эффективности реализации действующих политик безопасности операционных систем и систем управления базами данных. ОПК-16.4 Умеет анализировать результаты оценки эффективности реализации действующих политик безопасности операционных систем и систем управления базами данных; делать соответствующие выводы и строить свою деятельность в зависимости от достигнутых результатов и полученных выводов.
3	ОПК-17 Способен контролировать корректность функционирования программно-аппаратных средств защиты информации в компьютерных системах и сетях	ОПК-17.1 Владеет методами и средствами контроля корректности функционирования программно-аппаратных средств защиты информации в компьютерных системах и сетях. ОПК-17.2 Умеет применять на практике методы и средства контроля корректности функционирования программно-аппаратных средств защиты информации в компьютерных системах и сетях. ОПК-17.3 Умеет проводить дифференциацию и декомпозицию задач контроля корректности функционирования программно-аппаратных средств защиты информации в компьютерных системах и сетях. ОПК-17.4 Умеет анализировать результаты контроля корректности функционирования программно-аппаратных средств защиты информации в компьютерных системах и сетях; делать соответствующие выводы и строить свою деятельность в зависимости от достигнутых результатов и полученных выводов.
4	ПКО-11 Способен проводить проверки эффективности и выполнять работы по восстановлению работоспособности программных, программно-аппаратных и технических средств, подсистем защиты информации	ПКО-11.1 Обосновывает критерии и рассчитывает показатели эффективности защиты обрабатываемой информации. ПКО-11.2 Составляет методики тестирования, подбирает инструментарии? и осуществляет проверку эффективности функционирования программных, программно-аппаратных и технических средств, подсистем защиты информации. ПКО-11.3 Выполняет работы по восстановлению работоспособности программных, программно-

№ п/п	Код и название компетенции	Ожидаемые результаты
		аппаратных и технических средств, подсистем защиты информации.
5	ПКО-12 Способен выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности, проводить мониторинг и анализ эффективности реализации систем защиты информации и действующих политик безопасности в компьютерных системах	ПКО-12.1 Выполняет работы, связанные с реализацией частных политик информационной безопасности автоматизированной системы. ПКО-12.2 Проводит мониторинг и аудит безопасности компьютерной системы в сфере профессиональной деятельности. ПКО-12.3 Формирует основные показатели и критерии эффективности, оценивает эффективность компьютерной системы и ее средств защиты в области профессиональной деятельности.
6	ПКО-7 Способен проводить анализ информационной безопасности объектов и систем, принимать участие в организации и сопровождении аттестации объекта информатизации на предмет соответствия требованиям защиты информации	ПКО-7.1 Проводит анализ безопасности компьютерных систем, в том числе с использованием методов моделирования, на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности. ПКО-7.2 Участвует в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требовании? к уровню защищенности компьютерной системы. ПКО-7.3 Вырабатывает рекомендации в связи с проведенным анализом безопасности, в том числе для принятия решения о повторной аттестации компьютерной системы (в том числе автоматизированных систем), предложения по устранению выявленных уязвимостей.
7	ПКО-9 Способен участвовать в управлении информационной безопасностью компьютерной системы, разрабатывать предложения по ее совершенствованию	ПКО-9.1 Разрабатывает и организует выполнение мероприятий в соответствии с положениями политики информационной безопасности и защиты информации ограниченного доступа. ПКО-9.2 Разрабатывает предложения по совершенствованию системы управления информационной безопасностью компьютерной системы. ПКО-9.3 Разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ И АКАДЕМИЧЕСКИХ ЧАСАХ

4.1. Общая трудоемкость дисциплины составляет:

4 зачетные единицы (144 ак. ч.).

4.2. Распределение объема учебной дисциплины на контактную работу с преподавателем и самостоятельную работу обучающихся

	Количество часов	
Вид учебной работы	Всего по учебному плану	Семестр 8
Контактная работа	48	48,15
Аудиторные занятия (всего):	48	48
В том числе:		
лекции (Л)	32	32
практические (ПЗ) и семинарские (С)	16	16
Самостоятельная работа (всего)	60	60
Экзамен (при наличии)	36	36
ОБЩАЯ трудоемкость дисциплины, часы:	144	144
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	4.0	4.0
Текущий контроль успеваемости (количество и вид текущего контроля)	КР (1), ПК1, ПК2	КР (1), ПК1, ПК2
Виды промежуточной аттестации (экзамен, зачет)	ЭК	ЭК

4.3. Содержание дисциплины (модуля), структурированное по темам (разделам)

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
1	8	Раздел 1 КС и их организация / Сетевые атаки.	1				4	5	
2	8	Тема 1.1 Основные механизмы проведения сетевых атак на различных уровнях модели ISO/OSI	1				4	5	
3	8	Раздел 2 Механизмы реализации атак в сетях TCP/IP./	2		1		4	7	
4	8	Тема 2.1 Методы сканирования портов. Методы обнаружения пакетных снифферов. Методы обхода МЭ.	2		1		4	7	
5	8	Раздел 3 Методы перехвата сетевых соединений в сетях TCP/IP./	2		2		4	8	
6	8	Тема 3.1 Технические меры защиты от сетевых атак. Атаки направленные на сетевую инфраструктуру	2		2		4	8	
7	8	Раздел 4 Примеры сетевых атак в сетях TCP/IP.	5		1		8	14	ПК1, Устные опросы, выполнение практических заданий
8	8	Тема 4.1 Технические меры защиты от сетевых атак	1		1			2	
9	8	Тема 4.2 Принуждение к ускоренной передаче..	1				4	5	
10	8	Тема 4.3 Атаки,	1					1	

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		направленные на отказ в обслуживании.							
11	8	Тема 4.4 Изменение конфигурации и состояния хостов. Программно-технические меры защиты от сетевых атак	2					2	
12	8	Раздел 5 Криптографические методы защиты информации в компьютерных сетях.	5				12	17	
13	8	Тема 5.1 Криптографические протоколы обеспечения безопасности.	1				4	5	
14	8	Тема 5.2 Протоколы аутентификации на прикладном уровне. Протокол Kepberos.	2				4	6	
15	8	Тема 5.3 Протоколы аутентификации на транспортном уровне: протокол SSI/TLS/	2				4	6	
16	8	Раздел 6 Защита виртуальных частных сетей (VPN).	4		2		12	18	
17	8	Тема 6.1 Назначение, основные возможности и варианты реализации VPN.	1				4	5	
18	8	Тема 6.2 Достоинства и недостатки применения VPN	1				4	5	
19	8	Тема 6.3 Протокол IPSEC/ Протоколы AH и ESP.	1		2		4	7	
20	8	Тема 6.4	1					1	

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		Использование протокола L2TP для организации виртуальных частных сетей.							
21	8	Раздел 7 Разработка защищенных сетевых приложений.	3		2		8	13	
22	8	Тема 7.1 Аутентификация, шифрование, обеспечение целостности с использованием программного интерфейса SSPI.	2		2		4	8	
23	8	Тема 7.2 Программный интерфейс Open SSI.	1				4	5	
24	8	Раздел 8 Программно-аппаратные средства обеспечения безопасности в компьютерных сетях.	3		2			5	
25	8	Тема 8.1 Средства защиты локальных сетей при подключении к Интернет.	1		2			3	
26	8	Тема 8.2 Место и роль МЭ в обеспечении сетевой безопасности. Основные возможности и схемы развертывания МЭ	2					2	
27	8	Раздел 9 Методы сетевой трансляции адресов (NAT).	3		2		8	13	ПК2, Устный опрос, выполнение практических заданий
28	8	Тема 9.1 Построение правил фильтрации. Реализация сетевой политики	2		2			4	

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		безопасности с использованием МЭ.							
29	8	Тема 9.2 Методы обхода межсетевых экранов	1				4	5	
30	8	Раздел 10 Защита серверов и рабочих станций.	2		2			4	
31	8	Тема 10.1 Системы обнаружения вторжений (СОВ). Место и роль СОВ в общей системе обеспечения сетевой безопасности. Классификация СОВ.	2		2			4	
32	8	Раздел 11 Средства и методы предотвращения в обнаружении вторжений.	2		2			4	
33	8	Тема 11.1 Выявление атак на основе сигнатур атак и выявление аномалий. Аудит прикладных служб. Средства обнаружения уязвимостей сетевых служб. Системы виртуальных ловушек (Honey Pot и Paded Geet).	2		2			4	
34	8	Раздел 12 Курсовая работа						0	КР
35	8	Экзамен						36	ЭК
36		Всего:	32		16		60	144	

4.4. Лабораторные работы / практические занятия

Лабораторные работы учебным планом не предусмотрены.

Практические занятия предусмотрены в объеме 16 ак. ч.

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего часов/ из них часов в интерактивной форме
1	2	3	4	5
1	8	РАЗДЕЛ 2 Механизмы реализации атак в сетях TCP/IP./ Тема: Методы сканирования портов. Методы обнаружения пакетных снифферов. Методы обхода МЭ.	ПЗ 1 Инструментальные средства проведения атак	1
2	8	РАЗДЕЛ 3 Методы перехвата сетевых соединений в сетях TCP/IP./ Тема: Технические меры защиты от сетевых атак. Атаки направленные на сетевую инфраструктуру	ПЗ 2 Методы и средства перехвата в сетях TSP/IP	2
3	8	РАЗДЕЛ 4 Примеры сетевых атак в сетях TCP/IP. Тема: Технические меры защиты от сетевых атак	ПЗ 3 Технические меры защиты от сетевых атак	1
4	8	РАЗДЕЛ 6 Защита виртуальных частных сетей (VPN). Тема: Протокол IPSEC/ Протоколы AH и ESP.	ПЗ 4 Развертывание VPN с использованием IPSEC	2
5	8	РАЗДЕЛ 7 Разработка защищенных сетевых приложений. Тема: Аутентификация, шифрование, обеспечение целостности с использованием программного интерфейса SSPI.	ПЗ 5 Обеспечение целостного с использованием программного интерфейса SSPI	2

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего часов/ из них часов в интерактивной форме
1	2	3	4	5
6	8	РАЗДЕЛ 8 Программно-аппаратные средства обеспечения безопасности в компьютерных сетях. Тема: Средства защиты локальных сетей при подключении к Интернет.	ПЗ 6 Развертывание VPN базовыми средствами ОС Linux с использованием L2TP.	2
7	8	РАЗДЕЛ 9 Методы сетевой трансляции адресов (NAT). Тема: Построение правил фильтрации. Реализация сетевой политики безопасности с использованием МЭ.	ПЗ 7 Настройка и использование встроенного пакетного фильтра ОС Linux iptables.	2
8	8	РАЗДЕЛ 10 Защита серверов и рабочих станций. Тема: Системы обнаружения вторжений (СОВ). Место и роль СОВ в общей системе обеспечения сетевой безопасности. Классификация СОВ.	ПЗ 8 Настройка и использование прокси-сервера SQUID	2
9	8	РАЗДЕЛ 11 Средства и методы предотвращения в обнаружении вторжений. Тема: Выявление атак на основе сигнатур атак и выявление аномалий. Аудит прикладных служб. Средства обнаружения уязвимостей сетевых служб. Системы виртуальных ловушек (Honey Pot и Paded Geet).	ПЗ 9 Использование и настройка средства обнаружения вторжений Snort	2
			ВСЕГО:	16 / 0

4.5. Примерная тематика курсовых проектов (работ)

Курсовая работа является заключительным этапом в изучении дисциплины “Основы построения защищенных компьютерных сетей” и защищается в конце семестра.

Целью дисциплины “Основы построения защищенных компьютерных сетей” является

изучение и освоение основных средств обеспечения сетевой безопасности, включая средства мониторинга трафика. В этой связи, курсовые работы, тематика которых приведена ниже, должны более глубоко освоить предлагаемые технологии и приобрести навыки их практического внедрение в компьютерную сеть. Исходя из цели курсового проекта, можно выделить следующие темы:

1) Технология SIEM и ее функциональные возможности. Преимущества и недостатки по сравнению с другими решениями.
2) Сетевые пакетные фильтры и их разновидности.
3) Посредники и особенности их применения для сетевой защиты.
4) Технология NAT и варианты ее развития
5) Сеансовый посредник SoC и специфика его применения
6) Инспекторы состояния как инструмент фильтрации для обеспечения требуемого уровня ИБ.
7) Обеспечение межсетевой защиты ресурсов посредством UTM-устройств и NG firmware
8) Виртуальные частные сети и наиболее часто используемые протоколы VPN
9) Характеристика и архитектура протокола IPsec.
10) Системы обнаружения вторжений структуры и принципы построения
11) Сравнительный анализ систем обнаружения вторжений и для сетевой безопасности
12) DLP-системы и их возможности. Анализ часто применяемых DLP-систем.
13) Сетевые сканеры уязвимостей, как средства анализа защищенности сетей
14) Ловушки, как средство сбора информации о злоумышленнике.
15) Защита локальных вычислительных сетей от атак канального уровня
16) Защита информации от ПЭМИН
17) Обеспечение аутентификации пользователей и разграничение доступа к информационным ресурсам
18) Обеспечение защиты информационных ресурсов компании от сетевых атак
19) Построение систем безопасности сетевого уровня на базе протокола IPSec
20) Построение отказоустойчивой ЛВС на базе протокола STP
21) Защита рабочих станций сети от вредоносного ПО и несанкционированных действий сотрудников
22) Защита информации и конфиденциальных данных, передаваемых по e-mail
23) Система обнаружения вторжений RealSecure
24) Управление ключами в вычислительных системах
25) Инструментальные средства предотвращения сетевых атак

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины «Основы построения защищенных компьютерных систем» осуществляется в форме лекций, лабораторных работ и практических занятий.
В соответствии с требованиями ФГОС ВПО по направлению 10.05.01 «Компьютерная безопасность» с целью формирования и развития профессиональных навыков студентов предусмотрено использовать и проводить разбор презентаций лучших дипломных проектов по данной специализации. Кроме того, предусмотрены мастер-классы специалистов из:
- академии ФСБ
- компании «Информзащита»
- лаборатории Касперского
- РОСАТОМА

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Вид самостоятельной работы студента. Перечень учебно-методического обеспечения для самостоятельной работы	Всего часов
1	2	3	4	5
1	8	РАЗДЕЛ 1 КС и их организация / Сетевые атаки. Тема 1: Основные механизмы проведения сетевых атак на различных уровнях модели ISO/OSI	СР 1 Основные виды угроз для протоколов TCP/IP и OSI	4
2	8	РАЗДЕЛ 2 Механизмы реализации атак в сетях TCP/IP./ Тема 1: Методы сканирования портов. Методы обнаружения пакетных снифферов. Методы обхода МЭ.	СР 2 Методы сканирования портов	4
3	8	РАЗДЕЛ 3 Методы перехвата сетевых соединений в сетях TCP/IP./ Тема 1: Технические меры защиты от сетевых атак. Атаки направленные на сетевую инфраструктуру	СР 3 Технические меры защиты от сетевых атак.	4
4	8	РАЗДЕЛ 4 Примеры сетевых атак в сетях TCP/IP.	СР4 Подготовка к текущему контролю.	4
5	8	РАЗДЕЛ 4 Примеры сетевых атак в сетях TCP/IP. Тема 2: Принуждение к ускоренной передаче..	СР 4 Принуждение к ускоренной передаче	4
6	8	РАЗДЕЛ 5 Криптографические методы защиты информации в компьютерных сетях. Тема 1: Криптографические протоколы обеспечения безопасности.	СР 5 Современные средства в компьютерных сетях	4
7	8	РАЗДЕЛ 5 Криптографические методы защиты информации в компьютерных сетях. Тема 2: Протоколы аутентификации на	СР 5 Современные средства в компьютерных сетях	4

		прикладном уровне. Протокол Kepberos.		
8	8	РАЗДЕЛ 5 Криптографические методы защиты информации в компьютерных сетях. Тема 3: Протоколы аутентификации на транспортном уровне: протокол SSI/TLS/	СР 5 Современные средства в компьютерных сетях	4
9	8	РАЗДЕЛ 6 Защита виртуальных частных сетей (VPN). Тема 1: Назначение, основные возможности и варианты реализации VPN.	СР 6 Протоколы, обеспечивающую работу VPN	4
10	8	РАЗДЕЛ 6 Защита виртуальных частных сетей (VPN). Тема 2: Достоинства и недостатки применения VPN	СР 6 Протоколы, обеспечивающую работу VPN	4
11	8	РАЗДЕЛ 6 Защита виртуальных частных сетей (VPN). Тема 3: Протокол IPSEC/ Протоколы AH и ESP.	СР 6 Протоколы, обеспечивающую работу VPN	4
12	8	РАЗДЕЛ 7 Разработка защищенных сетевых приложений. Тема 1: Аутентификация, шифрование, обеспечение целостности с использованием программного интерфейса SSPI.	СР 7 Проблемы и реализация защиты сетевых приложений	4
13	8	РАЗДЕЛ 7 Разработка защищенных сетевых приложений. Тема 2: Программный интерфейс Open SSI.	СР 7 Проблемы и реализация защиты сетевых приложений	4
14	8	РАЗДЕЛ 9 Методы сетевой трансляции адресов (NAT).	СР 9 Подготовка к текущему контролю.	4
15	8	РАЗДЕЛ 9 Методы сетевой трансляции адресов (NAT). Тема 2: Методы обхода межсетевых	СР 9 Методы обхода межсетевых экранов	4

		экранов		
			ВСЕГО:	60

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Основная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
1	Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта	В.В. Яковлев, А.А. Корниенко	УМК МПС России, 2002 НТБ (уч.4); НТБ (фб.); НТБ (чз.1)	Все разделы
2	Компьютерные сети. Принципы, технологии, протоколы	В.Г. Олифер, Н.А. Олифер	"Питер", 2006 НТБ (уч.3)	Все разделы

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
3	Стандарты ИБ. Курс лекций	Галатенко В.А.	ИНТУИТ.РУ, Интернет-Университет Информ. Технологий М. , 2004	Все разделы
4	Безопасность корпоративных сетей	Биячуев Т.А.	СПБ, , 2006	Все разделы

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ "ИНТЕРНЕТ", НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Корниенко А.А. , Слюсаренко И.М., 2009 на сайте FORUM

9. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Требования к программному обеспечению и перечень информационных технологий используемых при прохождении учебной дисциплины

1. распространяемая система виртуализации Virtual Box.
2. Операционная система Linux.
3. Свободно распространяемый пакетный фильтр iptables.
4. Свободно распространяемый прокси-сервер SQUID.
5. Свободно распространяемые ПО для организации виртуальных сетей OPEN VPN.
6. Свободно распространяемая система обнаружения вторжений Snort.
7. Свободно распространяемый сервер удаленного доступа OPENSSH.

10. ОПИСАНИЕ МАТЕРИАЛЬНО ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Должно быть предусмотрено наличие компьютерного класса и интерактивная доска. Для практических занятий необходимо наличие компьютерного класса, объединенного в локальную вычислительную сеть. На компьютерах должны быть установлены серверные версии ОС Linux (или ОС в рамках виртуальных машин). В качестве коммуникационного оборудования могут использоваться коммутаторы, позволяющие организовать VLAN. Желательно доступ в Интернет. Желательно, чтобы студенты имели при себе носители информации (flash-накопители).

11. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

В процессе самостоятельной подготовки обучающиеся должны быть обеспечены доступом к сети интернет.
Активно использовать электронные образовательные ресурсы порталов:
- «Информзащита»
- «Эшелон»
- ФСТЭК РФ
- Лаборатории Касперского.

Для практического использования антивирусного ПО ресурс (http:/Knowledge.allbest.ru)