МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Забайкальский государственный университет»
(ФГБОУ ВО «ЗабГУ»)

Энергетический факультет
Кафедра Физики и техники связи

УТВЕРЖДАЮ:

Декан факультета

Энергетический факультет

Батухтин Андрей Геннадьевич

«____»_____20____ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.ДВ.02.01 Защита информационных ресурсов в компьютерных сетях
на 144 часа(ов), 4 зачетных(ые) единиц(ы)
для направления подготовки (специальности) 11.04.02 - Инфокоммуникационные технологии и системы связи

составлена в соответствии с ФГОС ВО, утвержденным приказом Министерства образования и науки Российской Федерации от «___» _____ 20____ г. №____

Профиль – Безопасность инфокоммуникационных систем и сетей (для набора 2023)
Форма обучения: Очная

1. Организационно-методический раздел

1.1 Цели и задачи дисциплины (модуля)

Цель изучения дисциплины:

является формирование у студентов знаний и умений по защите компьютерных сетей с применением современных программно-аппаратных средств.

Задачи изучения дисциплины:

дать знания: • о методах и средствах защиты информации в компьютерных сетях; • о технологии межсетевого экранирования; • о методах и средствах построения виртуальных частных сетей; • о методах и средствах аудит уровня защищенности информационных систем. Приобретенные знания и навыки позволят студентам работать в должностях администраторов компьютерных сетей и администраторов безопасности.

1.2. Место дисциплины (модуля) в структуре ОП

Дисциплина «Защита информационных ресурсов в компьютерных сетях» входит в состав базовой части модуля «Б». Дисциплина изучается на 1 курсе в 1 семестре.

1.3. Объем дисциплины (модуля) с указанием трудоемкости всех видов учебной работы

Общая трудоемкость дисциплины (модуля) составляет 4 зачетных(ые) единиц(ы), 144 часов.

Виды занятий	Семестр 1	Всего часов
Общая трудоемкость		144
Аудиторные занятия, в т.ч.	34	34
Лекционные (ЛК)	17	17
Практические (семинарские) (ПЗ, СЗ)	17	17
Лабораторные (ЛР)	0	0
Самостоятельная работа студентов (СРС)	74	74
Форма промежуточной аттестации в семестре	Экзамен	36
Курсовая работа (курсовой проект) (КР, КП)		

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы		Планируемые результаты обучения по дисциплине
Код и наименование компетенции	Индикаторы достижения компетенции, формируемые в рамках дисциплины	Дескрипторы: знания, умения, навыки и (или) опыт деятельности
ПК-4	ПК-4.1 Знает общие принципы функционирования и архитектуру аппаратных, программных и программноаппаратных средств администрируемой сети	Знать: архитектуры и возможности системы безопасности ОС Windows XP/7/2008 R2; Уметь: умеет использовать возможности системы безопасности ОС Windows XP/7/2008 R2; Владеть: навыками развертывания и применения инфраструктуры открытых ключей (PKI) для обеспечения безопасности ОС и приложений;
ПК-4	Умеет пользоваться контрольно-измерительными приборами и аппаратурой; конфигурировать операционные системы сетевых устройств, производить мониторинг администрируемой сети	Знать: - используемые в ОС Windows XP/7/2008 R2 протоколы аутентификации, их достоинства и недостатки; - Об управлении учетными записями пользователей и групп в целях обеспечения безопасности; Уметь: пользоваться контрольно-измерительными приборами и аппаратурой;производить мониторинг администрируемой сети Владеть: конфигурацией операционной системы сетевых устройств,

ПК-4	Умеет устанавливать и инициализировать новое программное обеспечение	Знать: - уязвимости ОС Windows XP/7/2008 R2 и методы их устранения; - проблемы и особенности применения файловой системы с шифрованием (EFS), способы повышения уровня безопасности при использовании EFS. Уметь: использовать рекомендации Microsoft, NIST, NSA и других организаций по настройке средств безопасности Windows XP/7/2008 R2; Владеть: навыками конфигурирования сетевых устройств и операционных систем
ПК-5	ПК-5.1 Знает основы обеспечения информационной безопасности, нормативные правовые акты в области информационной безопасности, системное программное обеспечение, включая знания о типовых уязвимостях	Знать: особенности реализации технологий обеспечения безопасности (инфраструктура открытых ключей, виртуальные частные сети, Уметь: применять дополнительные инструменты и утилиты для управления системой безопасности ОС Windows XP/7/2008 R2; Владеть: навыками настройки средств защиты сетевого трафика в локальной сети и при организации удаленного доступа (IPSec, L2TP, SSTP, SSL/TLS);
ПК-5	ПК-5.3 Умеет осуществлять сбор и анализ исходных данных для обеспечения информационной	Знать: об управлении учетными записями пользователей и групп в целях обеспечения безопасности;

	безопасности системного программного обеспечения	Уметь: использовать механизмы групповых политик для централизованной настройки безопасных конфигураций рабочих станций и серверов. Владеть: навыками ограниченного применения съемных USB носителей в Windows XP/7/2008 R2.
ПК-5	Владеет навыками установки и настройки аппаратно-программных средств защиты системного программного обеспечения	Знать: проблемы и особенности применения файловой системы с шифрованием (EFS), способы повышения уровня безопасности при использовании EFS. Уметь: применять программно-аппаратные средства защиты информации Владеть: навыками установки и настройки аппаратно-программных средств защиты системного программного обеспечения

3. Содержание дисциплины

3.1. Разделы дисциплины и виды занятий

3.1 Структура дисциплины для очной формы обучения

Модуль	Номер раздела	Наименование раздела	Темы раздела	Всего часов	Аудиторные занятия			СРС
					ЛК	ПЗ (СЗ)	ЛР	
1	1.1	Защитные механизмы	Введение.Защитные механизмы. Доверительные отношения. Контроллеры домена. Подразделения.	26	4	4	0	18

			Учетные записи пользователей и компьютеров					
2	2.1	Группы	Группы. Групповые политики Настройки групповой политики.	26	4	4	0	18
3	3.1	Идентификация. Маркер доступа.	Клонирование. Права и привилегии пользователей. Аутентификация. Протоколы аутентификации. Методы аутентификации.	26	4	4	0	18
4	4.1	Защита подсистемы аутентификации. Обеспечение безопасности учетных записей.	Компоненты системы безопасности Windows 2003/2008 R2	30	5	5	0	20
Итого				108	17	17	0	74

3.2. Содержание разделов дисциплины

3.2.1. Лекционные занятия, содержание и объем в часах

Модуль	Номер раздела	Тема	Содержание	Трудоемкость (в часах)
1	1.1	Введение. Защитные механизмы. Контроль целостности и нформационн ых ресурсов. Управление защитными механизмами.	Архитектура Active Directory. Доверительные отношения. Контроллеры домена для чтения. Подразделения. Учетные записи пользователей и компьютеров.	4
2	2.1	Группы. Объекты групповой политики.	Группы. Объекты групповой политики. Управление локальными групповыми политиками в системе Windows Vista/7/2008	2
	2.1	Технология	Новый формат шаблонов для	2

		настроек групповой политики (Group Policy Preferences).	групповых политик в Windows Vista/7/2008	
3	3.1	Идентификация.Именование субъектов и объектов. Маркер доступа (Security Access Token).	Нулевые сеансы в Windows. Субъекты доступа. Проблемы идентификации.Протоколы аутентификации, используемые в Windows. Протокол Lan Manager (LM). Протокол NTLMv2. Сравнение алгоритмов аутентификации. Аутентификация при удаленном доступе: протоколы CHAP, MS-CHAP, MS-CHAPv.2, EAP.	4
4	4.1	Парольная политика.	Повышение безопасности учетной записи администратора. Обеспечение безопасности гостевой учетной записи. Обход аутентификации при физическом доступе к компьютеру.. Архитектура системы безопасности. Регистрация пользователя вне домена. Локальная база данных учетных записей.	5

3.2.2. Практические занятия, содержание и объем в часах

Модуль	Номер раздела	Тема	Содержание	Трудоемкость (в часах)
1	1.1	Добавление ПК в домен Active Directory.	Добавление ПК в домен Active Directory.	4
2	2.1	Создание групповой политики в Windows Server 2008 R2	Создание групповой политики в Windows Server 2008 R2 Создание в домене Active Directory организационного подразделения, учетной записи пользователя и группы	4
3	3.1	Изучение идентификаторов безопасности. Инвентаризация пользователей	Перехват паролей пользователей по сети. Перехват и компрометация пароля Kerberos V5 по сети. Изучение работы контроля учетных записей (UAC) при помощи встроенных средств Windows.	4

		ПК при идент ификаторов безопасности.	Изучение работы уровней User Account Control (UAC) на Windows 7 и на Windows Vista.. Восстановление паролей из хешей LAN Manager и NTLM. Настройка NTLM2 и запрет хранения LM хешей.	
4	4.1	Атака на кэш паролей. Защита от атаки кэш паролей.	Сброс пароля локального администратора при помощи продуктов Microsoft. Сброс пароля локального администратора при помощи продуктов сторонних производителей. Интерактивная регистрация в домене.	5

3.2.3. Лабораторные занятия, содержание и объем в часах

Модуль	Номер раздела	Тема	Содержание	Трудоемкость (в часах)

3.3. Содержание материалов, выносимых на самостоятельное изучение

Модуль	Номер раздела	Содержание материалов, выносимого на самостоятельное изучение	Виды самостоятельной деятельности	Трудоемкость (в часах)
1	1.1	Введение. Криптографическое закрытие хранимых и передаваемых по каналам данных. Active Directory и система безопасности. Новые возможности Active Directory в Windows Server 2008 R2	Составление конспекта	18
2	2.1	Объекты групповых политик.Новый формат шаблонов для групповых политик в Windows Vista/7/2008	составление конспекта	18
3	3.1	Изменения в маркерах безопасности в Windows Vista и выше. Использование ключа	Составление конспекта	18

		реестра RestrictAnonymous в Windows 2000/XP/2003. Протоколы аутентификации, используемые в Windows. Протокол Lan Manager (LM). Протокол NTLMv2. Сравнение алгоритмов аутентификации. Аутентификация при удаленном доступе: протоколы CHAP, MS-CHAP, MS-CHAPv.2, EAP.		
4	4.1	Парольная политика. Повышение безопасности учетной записи администратора. Обеспечение безопасности гостевой учетной записи. Обход аутентификации при физическом доступе к компьютеру. Архитектура системы безопасности. Регистрация пользователя вне домена. Локальная база данных учетных записей.Интерактивная регистрация в домене.	Составление конспекта	20

4. Фонд оценочных средств для проведения текущей и промежуточной аттестации обучающихся по дисциплине

Фонд оценочных средств текущего контроля и промежуточной аттестации по итогам освоения дисциплины представлен в приложении.

Фонд оценочных средств

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Основная литература

5.1.1. Печатные издания

1. 1. Хорев П.Б. Методы и средства защиты информации в компьютерных системах : учеб. пособие. - 4-е изд., стер. - Москва : Академия, 2008. - 256 с. - (Высшее профессиональное образование). - ISBN 978-5-7695-5118-5 : 289-79. 2. Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : учеб. пособие. - Москва : Академия, 2006. - 240с. - (Высшее профессиональное образование). - ISBN 5-7695-2706-4 : 291-40. 3. Мельников Владимир Павлович. Информационная безопасность и защита информации : учеб. пособие для студентов высш. учеб. заведений / под ред. С.А. Клейменова. - 3-е изд., стер. - Москва : Академия, 2008. - 336с. - ISBN 978-5-7695-4884-0 : 390-39.

5.1.2. Издания из ЭБС

1. 1. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : Рекомендовано Государственным образовательным учреждением высшего профессионального образования "Академия Федеральной службы безопасности Российской Федерации" в качестве учебного пособия для студентов высших учебных заведений, обучающихся по специальностям направления подготовки 090300 - "Информационная безопасность вычислительных, автоматизированных и телекоммуникационных систем" и направлению подготовки 090900 - "Информационная безопасность". Регистрационный номер рецензии № 742 от 25 февраля 2010 г. (ГОУВПО "Московский государственный университет печати") / Девянин П.Н. - Moscow : Горячая линия - Телеком, 2012. - . - Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс] : Учебное пособие для вузов / Девянин П.Н. - М. : Горячая линия - Телеком, 2012. - http://www.studentlibrary.ru/book/ISBN9785991201476.html. - ISBN 978-5-9912-0147-6.

5.2. Дополнительная литература

5.2.1. Печатные издания

1. 1. Клейменов Сергей Анатольевич. Администрирование в информационных системах : учеб. пособие / под ред. В.П. Мельникова. - Москва : Академия, 2008. - 272с. - (Высшее профессиональное образование). - ISBN 978-5-7695-4708-9 : 196-46. 2. Расторгуев С.П. Основы информационной безопасности : учеб. пособие для студентов вузов. - Москва : Академия, 2007. - 186 с. - (Высш. проф. образование). - ISBN 978-5-7695-3098-2 : 225-00.

5.2.2. Издания из ЭБС

1. 1. Милославская Н.Г.Проверка и оценка деятельности по управлению информационной безопасностью : Допущено Учебно-методическим объединением высших учебных заведений России по образованию в области информационной безопасности в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению подготовки 090900 - "Информационная безопасность" (уровень - магистр) / Милославская Н.Г.; Сенаторов М.Ю.; Толстой А.И. - Moscow : Горячая линия - Телеком, 2013. - . - Проверка и оценка деятельности по управлению информационной безопасностью [Электронный ресурс] : Учебное пособие для вузов / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - Вып. 5. - М. : Горячая линия - Телеком, 2013. - (Серия "Вопросы управления

информационной безопасностью"). - http://www.studentlibrary.ru/book/ISBN9785991202756.html. - ISBN 978-5-9912-0275-6.

5.3. Базы данных, информационно-справочные и поисковые системы

Название	Ссылка
Единое окно доступа к образовательным ресурсам	http://window.edu.ru/
Электронно-библиотечная система «eLibrary»:	http://www.elibrary.ru
Электронно-библиотечная система «Буквоед»:	http://91.189.237.198:8778/poisk2.aspx
Электронная библиотека диссертаций РГБ:	https://diss.rsl.ru/
сайт национального открытого университета;	https://www.intuit.ru/
IT-портал «Сервер Информационных Технологий»;	http://citforum.ru/
ресурс для IT-специалистов, издаваемый компанией «ТМ»	https://habrahabr.ru/
сайт вопросов и ответов для IT-специалистов;	http://stackoverflow.com/
сайт проекта «Развитие Бизнеса / Ру»;	http://www.devbusiness.ru
онлайн-версия информационно-правовой системы "КонсультантПлюс"	http://www.consultant.ru/
Открытая база ГОСТов	http://standartgost.ru/

6. Перечень программного обеспечения

Программное обеспечение общего назначения: ОС Microsoft Windows, Microsoft Office, ABBYY FineReader, ESET NOD32 Smart Security Business Edition, Foxit Reader, АИБС "МегаПро".

Программное обеспечение специального назначения:

1) 1С-Битрикс: Корпоративный портал - Компания 1С: Предприятие 8. Комплект для обучения в высших и средних учебных заведениях 7-Zip ABBYY FineReader Adobe Audition Adobe Flash Adobe In Design Adobe Lightroom Adobe Photoshop

2) Имитационная программа модульного конструктора цифрового стенда

7. Материально-техническое обеспечение дисциплины

Наименование помещений для проведения учебных занятий и для самостоятельной работы обучающихся	Оснащенность специальных помещений и помещений для самостоятельной работы
Учебные аудитории для проведения занятий лекционного типа	Состав оборудования и технических средств обучения указан в паспорте аудитории, закрепленной расписанием по факультету
Учебные аудитории для проведения практических занятий	
Учебные аудитории для промежуточной аттестации	
Учебные аудитории для текущей аттестации	Состав оборудования и технических средств обучения указан в паспорте аудитории, закрепленной расписанием по кафедре

8. Методические рекомендации по организации изучения дисциплины

Методические рекомендации по подготовке к лекционным занятиям. В ходе лекционных занятий необходимо вести конспектирование учебного материала. Перед каждым лекционным занятием студенту рекомендуется ознакомиться с составленными конспектами, документацией языка программирования, а также прочитать соответствующие разделы из рекомендованных источников.
Методические рекомендации по подготовке к практическим занятиям. Целью практических занятий является углубление и закрепление теоретических знаний, полученных студентами на лекциях и в процессе самостоятельного изучения учебного материала, а, следовательно, формирование у них определенных умений и навыков.
Методические рекомендации по организации самостоятельной работы. Самостоятельная работа приводит студента к получению нового знания, упорядочению и углублению имеющихся знаний, формированию у него профессиональных навыков и умений. Самостоятельная работа выполняет ряд функций: развивающую; информационно-обучающую; ориентирующую и стимулирующую; воспитывающую; исследовательскую. Это и позволяет сформировать нужные компетенции в ходе изучения дисциплины.
Студентам рекомендуется с самого начала освоения курса работать с литературой и предлагаемыми заданиями в форме подготовки к очередному аудиторному занятию. При этом актуализируются имеющиеся знания, а также создается база для усвоения нового материала, возникают вопросы, ответы на которые студента получает в аудитории.
Можно отметить, что некоторые задания для самостоятельной работы по курсу имеют определенную специфику.

Разработчик/группа разработчиков:
Татьяна Витальевна Кузьмина

Типовая программа утверждена

Согласована с выпускающей кафедрой
Заведующий кафедрой
_____ «___»_____20____г.