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

Мирошников С.Ф.

«____»_____20____г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.Б.26.Защита информационных ресурсов в компьютерных сетях

на 216 часа(ов), 6 зачетных(ые) единиц(ы)

для направления подготовки (специальности) 10.05.02 – Информационная безопасность телекоммуникационных систем

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

Специализация – Защита информации в системах связи и управления (для набора 2020)

Форма обучения очная

1. Организационно-методический раздел

1.1 Цель и задачи дисциплины (модуля)

Цель изучения дисциплины:

Целью дисциплины «Защита информационных ресурсов в компьютерных сетях» является формирование у студентов знаний и умений по защите компьютерных сетей с применением современных программно-аппаратных средств.

Задачи изучения дисциплины:

Задачи 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 5 курсе в 9 семестре.

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

Общая трудоемкость дисциплины (модуля) составляет 6 зачетных(ые) единиц(ы), 216 часов.

Очная форма

Виды занятий	Распределение по семестрам	Всего часов
	9 семестр	
Общая трудоемкость		216
Аудиторные занятия, в т.ч.	68	68
лекционные (ЛК)	34	34
практические (семинарские) (ПЗ, СЗ)	17	17
лабораторные (ЛР)	17	17
Самостоятельная работа студентов (СРС)	112	112
Форма промежуточной аттестации в семестре	Экзамен	36
Курсовая работа (курсовой проект) (КР, КП)		

2. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Индекс компетенции	Содержание компетенции
ПК-1	Способность осуществлять анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем
ПК-9	Способность участвовать в проведении аттестации телекоммуникационных систем по требованиям защиты информации
ПК-15	Способность проводить инструментальный мониторинг защищенности телекоммуникационных систем, обеспечения требуемого качества обслуживания
ПСК-10.1	Способность применять теорию сигналов и систем для анализа телекоммуникационных систем и оценки их помехоустойчивости
ПСК-10.2	Способность формировать технические задания и участвовать в разработке аппаратных и программных средств защиты телекоммуникационных систем
ПСК-10.3	Способность оценивать возможности средств технических разведок в отношении к системам связи, управления и объектами информатизации
ПСК-10.4	Способность применять наиболее эффективные методы и средства для закрытия возможных каналов перехвата акустической речевой информации
ПСК-10.5	Способность проводить оценку уровня защищенности и обеспечивать эффективное применение средств защиты информационных ресурсов компьютерных сетей и систем беспроводной связи

Планируемые результаты обучения по дисциплине для последовательного достижения уровней сформированности компетенций

Результат обучения

Знать	Пороговый: 1. архитектуры и возможности системы безопасности ОС Windows XP/7/2008 R2; 2.Особенности реализации технологий обеспечения безопасности (инфраструктура открытых ключей, виртуальные частные сети, система однократного ввода пароля)
	Стандартный: 3.используемые в ОС Windows XP/7/2008 R2 протоколы аутентификации, их достоинства и недостатки; 4. Об управлении учетными записями пользователей и групп в целях обеспечения безопасности;
	Эталонный: 5. уязвимости ОС Windows XP/7/2008 R2 и методы их устранения; 6. проблемы и особенности применения файловой системы с шифрованием (EFS), способы повышения уровня безопасности при использовании EFS.
Уметь	Пороговый: 1. использовать рекомендации Microsoft, NIST, NSA и других организаций по настройке средств безопасности Windows XP/7/2008 R2;
	Стандартный: 2. применять дополнительные инструменты и утилиты для управления системой безопасности ОС Windows XP/7/2008 R2;
	Эталонный: 3. использовать механизмы групповых политик для централизованной настройки безопасных конфигураций рабочих станций и серверов.
	Пороговый: 1. навыками развертывания и применения инфраструктуры открытых ключей (PKI) для обеспечения безопасности ОС и приложений;

Владеть	Стандартный: 2. навыками настройки средств защиты сетевого трафика в локальной сети и при организации удаленного доступа (IPSec, L2TP, SSTP, SSL/TLS);
	Эталонный: 3.навыками ограниченного применения съемных USB носителей в Windows XP/7/2008 R2.

3. Содержание дисциплины

3.1. Разделы дисциплины и виды занятий

Очная форма

Модуль	Номер раздела	Наименование раздела	Всего часов	Аудиторные занятия			СРС
				ЛК	ПЗ(СЗ)	ЛР	
1	1	Введение.Защитные механизмы. Доверительные отношения. Контроллеры домена.	24	6	2	2	14
	2	Подразделения. Учетные записи пользователей и компьютеров	22	4	2	2	14
2	3	Группы.Групповые политики.	22	4	2	2	14
	4	Настройки групповой политики.	22	4	2	2	14
3	5	Идентификация. Маркер доступа. Клонирование. Права и привилегии пользователей.	22	4	2	2	14
	6	Аутентификация. Протоколы аутентификации. Методы аутентификации.	22	4	2	2	14
4	7	Защита подсистемы аутентификации. Обеспечение безопасности учетных записей.	22	4	2	2	14
	8	Компоненты системы безопасности Windows 2003/2008 R2	24	4	3	3	14
Итого			180	34	17	17	112

3.2. Лекционные занятия

Очная форма

Модуль	Номер раздела	Содержание лекционных занятий
1	1	Введение. Защитные механизмы. Контроль целостности информационных ресурсов. Управление защитными механизмами. Архитектура Active Directory. Доверительные отношения. Контроллеры домена для чтения.
	2	Подразделения. Учетные записи пользователей и компьютеров.
2	3	Группы. Объекты групповой политики. Управление локальными групповыми политиками в системе Windows Vista/7/2008
	4	Технология настроек групповой политики (Group Policy Preferences). Новый формат шаблонов для групповых политик в Windows Vista/7/2008
3	5	Идентификация.Именование субъектов и объектов. Маркер доступа (Security Access Token). Нулевые сеансы в Windows. Субъекты доступа. Проблемы идентификации.
	6	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	7	Парольная политика. Повышение безопасности учетной записи администратора. Обеспечение безопасности гостевой учетной записи. Обход аутентификации при физическом доступе к компьютеру.
	8	Архитектура системы безопасности. Регистрация пользователя вне домена. Локальная база данных учетных записей.

3.3. Практические (семинарские) занятия

Очная форма

Модуль	Номер раздела	Содержание практических(семинарских) занятий

1	1	Добавление ПК в домен Active Directory.
2	3	Создание групповой политики в Windows Server 2008 R2
3	5	Изучение идентификаторов безопасности. Инвентаризация пользователей ПК при идентификаторов безопасности.
	6	Перехват паролей пользователей по сети. Перехват и компрометация пароля Kerberos V5 по сети.
4	7	Атака на кэш паролей. Защита от атаки кэш паролей.

3.4. Лабораторные занятия

Очная форма

Модуль	Номер раздела	Содержание лабораторных занятий
1	1	Создание сети предприятия на базе Active Directory
2	3	Создание в домене Active Directory организационного подразделения, учетной записи пользователя и группы
3	5	Изучение работы контроля учетных записей (UAC) при помощи встроенных средств Windows. Изучение работы уровней User Account Control (UAC) на Windows 7 и на Windows Vista.
	6	Восстановление паролей из хешей LAN Manager и NTLM. Настройка NTLM2 и запрет хранения LM хешей.
4	7	Сброс пароля локального администратора при помощи продуктов Microsoft. Сброс пароля локального администратора при помощи продуктов сторонних производителей.
	8	Интерактивная регистрация в домене.

3.5. Организация самостоятельной работы

Очная форма

Модуль	Номер раздела	Содержание материала выносимого на самостоятельное изучение	Виды самостоятельной работы
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
2	3	Объекты групповых политик.Новый формат шаблонов для групповых политик в Windows Vista/7/2008	устный опрос
3	5	Изменения в маркерах безопасности в Windows Vista и выше. Использование ключа реестра RestrictAnonymous в Windows 2000/XP/2003	составление конспекта
3	6	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.	устный опрос
4	7	Парольная политика. Повышение безопасности учетной записи администратора. Обеспечение безопасности гостевой учетной записи. Обход аутентификации при физическом доступе к компьютеру.	Подготовка докладов
4	8	Архитектура системы безопасности. Регистрация пользователя вне домена. Локальная база данных учетных записей.Интерактивная регистрация в домене.	консультация

4. Интерактивные формы образовательных технологий

Модуль	Номер раздела	Вид учебных занятий	Образовательные технологии	Количество часов
1-4	1-9	ЛР	Ситуационные задачи Технологии учебно-исследовательской деятельности (проведение, презентация и обсуждение микроисследований)	18
3	3	ЛК	Видеоэкскурсии	4

5. Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Основная литература

6.1.1. Печатные издания

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.

6.1.2. Издания из ЭБС

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.

6.2. Дополнительная литература

6.2.1. Печатные издания

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.

6.2.2. Издания из ЭБС

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.

6.3. Базы данных, информационно-справочные и поисковые системы

Единое окно доступа к образовательным ресурсам: http://window.edu.ru/

7. 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:

8. Материально-техническое обеспечение дисциплины

672000, г. Чита, ул. Кастринская-1, Ауд. 08-210. Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации . Комплект специализированной учебной мебели. Доска маркерная. Комплект мобильного оборудования, который организован в виде мобильного передвижного многофункционального комплекса (устанавливается в аудитории по заявке преподавателя): ноутбук, мультимедийный проектор, экран.
672000, г. Чита, ул. Кастринская-1, Ауд. 08-310а. Лаборатория программно-аппаратных средств обеспечения защиты информации. Учебная аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Рабочие места с антивирусными программными комплексами и аппаратными средствами аутентификации пользователя. Оборудование по защите информации от утечки по акустическому, акустоэлектрическим каналам, каналу побочных электромагнитных излучений и наводок, техническими средствами контроля эффективности защиты информации от утечки по указанным каналам. Мультимедийный к-т в составе: переносной экран на треноге, мультимедиапроектор, ноутбук. Комплект специальной учебной мебели. Доска маркерная. Доступ к сети Интернет и обеспечение доступа в электронную информационно-образовательную среду организации. Оборудование криптозащиты – HW-100 , АРМ VipNet клиент (12 лицензий) учебная защищенная сеть.
672000, г. Чита, ул. Кастринская-1, Ауд. 08-20. Лаборатория систем коммутации. Комплект специальной учебной мебели. Стойка Hyperline, ASCON Energy Sustems, ЦАТС МС 240 Зав.№403, кабельрост ПВМ администратора станции. Доступ к сети Интернет и обеспечение доступа в электронную информационно-образовательную среду организации. Переносной мультимедийный к-т в составе: экран на треноге, мультимедиапроектор, ноутбук.
672000, г. Чита, ул. Кастринская-1, Ауд. 08-310. Кабинет информатики и Интернет-технологий . Лаборатория мультисервисных сетей . Учебная аудитория для проведения занятий семинарского типа, курсового и дипломного проектирования, научно-исследовательской работы, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, самостоятельной работы обучающихся. Рабочие места на базе вычислительной техники и абонентские устройства, подключенные к сети «Интернет» с использованием проводных и/или беспроводных технологий, с установленным офисным пакетом и набором необходимых для проведения исследований дополнительных аппаратных и(или) программных средств, а также оборудованием для печати. Обеспечение доступа в электронную информационно-образовательную среду организации. Переносной мультимедийный к-т в составе: экран на треноге, мультимедиапроектор, ноутбук. Комплект специальной учебной мебели. Стойка Hyperline, ASCON Energy Sustems, ЦАТС МС 240 Зав.№403.

9. Методические рекомендации по организации изучения дисциплины

Лекции являются основным источником теоретического материала по дисциплине

«Физические основы электроники». Посещение и конспектирование лекций является обязательной составляющей успешного освоения дисциплины обучающимися.
Для эффективного освоения материала дисциплины «Физические основы электроники» необходимо выполнение следующих требований:
- обязательное посещение всех лекционных и практических занятий, способствующее системному овладению материалом курса;
- все вопросы соответствующих разделов и тем по дисциплине необходимо фиксировать (на любых носителях информации);
- обязательное выполнение домашних заданий является важнейшим требованием и условием формирования целостного и системного знания по дисциплине;
- обязательность личной активности каждого студента на всех занятиях по дисциплине;
- в случаях неясности каких-либо вопросов, обсуждаемых на занятиях, необходимо задать соответствующие вопросы преподавателю, а не оставлять их непонятыми;
- в случаях пропусков занятий по уважительным причинам студентам предоставляется право подготовки и представления заданий и ответов на вопросы изученного материала,с расчетом на помощь преподавателя в его усвоении;
- в случаях пропусков без уважительной причины студент обязан самостоятельно изучить соответствующий материал;
- необходимым условием является самостоятельность и инициативность студентов при контроле набора баллов по дисциплине для успешного прохождения промежуточной аттестации.
Порядок организации лабораторной работы студентов
Лабораторная работа студентов предполагает сознательной активной работы не только в лаборатории при сборке установки и проведении измерений, но и дома при подготовке к измерениям, обработке результатов и составления отчета.
Выполнение лабораторной работы есть определенная последовательность действий:
— подготовка к эксперименту;
— проведение измерений;
— обработка полученных результатов;
— формулировка выводов и написание отчета.
Для грамотного и быстрого их выполнения должна сложиться определенная система знаний и умений (ориентировочная основа действия), которая обеспечит правильное и рациональное исполнение действия.
Поэтому выполнение каждой лабораторной работы необходимо начинать с изучения ее описания и приведения знаний в систему, а именно:
— ясно представить себе общую цель данной конкретной лабораторной
работы и последовательность задач, решение которых приведет к достижению окончательной цели;
— знать основные особенности объекта исследования
— изучить и уметь объяснить физические основы используемых в работе методов измерения искомых величин;
— уметь нарисовать принципиальную схему используемой установки и знать назначение каждого из ее узлов;
— знать последовательность выполнения этапов лабораторной работы;— иметь общее представление об ожидаемых результатах проводимого эксперимента и
уметь выбрать метод, нужный для их математической обработки
О т ч е т с т у д е н т а п о р а б о т е д о л ж е н б ы т ь индивидуальным, составленным по
установленной форме, и содержать следующие разделы: наименование работы; цель работы; индивидуальное задание; применяемая аппаратура; е е описание (система, класс, цена давления и т.д.); краткое изложение методики, схемы опытов; таблицы данных измерений; итог обработки результатов и расчетные формулы; графики; анализ результатов и погрешностей; фрагмент конструкции соединения. Анализ результатов является важной частью отчета.
Порядок организации студентов на практическом занятии
Перед практическими занятиями студент должен повторить лекционный материал, ответив н а вопросы д л я самоконтроля п о необходимой теме, а также просмотреть рекомендации по решению типичных задач этой темы.
На практических занятиях обобщаются и систематизируются знания, полученные на

лекционных занятиях и формируются умения решать типовые задачи. При решении студент должен уметь:
- выделять описываемое явление (объект), анализировать условие задачи;
- выполнять построение модели явления;
- формулировать выводы из модели;
- выявлять применения полученных знаний в профессиональной деятельности.
Н а практических занятиях студент приобретает учится собирать и анализировать информацию для формирования исходных данных для проектирования средств и сетей связи.
Порядок организации самостоятельной работы студентов
Самостоятельная работа – индивидуальная учебная деятельность, осуществляемая без непосредственного руководства преподавателя, в ходе которой бакалавр активно воспринимает, осмысливает информацию, решает теоретические и практические задачи. В процессе проведенной самостоятельной работы формируются компетенции.Самостоятельная работа студентов предполагает:
- самостоятельный поиск, обработку (анализ, синтез, обобщение и систематизацию),адаптацию необходимой по дисциплине информации;
- выполнение заданий для самостоятельной работы;
- изучение и усвоение теоретического материала, представленного на лекционных занятиях и в соответствующих литературных источниках (рекомендуемая основная и дополнительная литература);
- самостоятельное изучение отдельных вопросов курса;
- подготовка к практическим и лабораторным занятиям, в соответствии с рекомендациями преподавателя (выполнение конкретных заданий, соответствующие организационные действия и т.д.).
Самостоятельное выполнение контрольных и лабораторных работ является основным средством освоения теоретического материала курса и приобретения умений и навыков его практического применения, поскольку только применение знаний обеспечивает их глубокое понимание. Контроль за самостоятельной работой производится на практических занятиях.

Разработчик/группа разработчиков: Ситников Павел Юрьевич, доцент

Рассмотрена на заседании кафедры
(протокол от 24.05.2019 г. № 16)