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.35.07.Методы и средства обеспечения критической информационной инфраструктуры

на 144 часа(ов), 4 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 обучить студентов принципам обеспечения информационной безопасности государства, организации, отдельного гражданина подходам к анализу ее информационной инфраструктуры и решению задач обеспечения информационной безопасности компьютерных систем. Дисциплина " Методы и средства обеспечения критической информационной инфраструктуры" имеет также целью содействовать фундаментализации образования, формированию научного мировоззрения и развитию системного мышления.
Задачи изучения

Задачи изучения дисциплины:

- приобретение обучаемыми необходимого объема знаний в области защита информации в современных компьютерных сетях;
- приобретение обучаемыми практических навыков в области данной области знаний: настройки специального ПО, организации работы и разграничения полномочий пользователей;
- формирование у обучаемых целостного представления комплексной защите компьютерных сетей.

1.2. Место дисциплины (модуля) в структуре ОП

Учебная дисциплина «Методы и средства обеспечения критической информационной инфраструктуры» является обязательной, входит в блок Б1.Б.35.07

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

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

Очная форма

Виды занятий	Распределение по семестрам	Всего часов
	11 семестр	
Общая трудоемкость		144
Аудиторные занятия, в т.ч.	55	55
лекционные (ЛК)	22	22
практические (семинарские) (ПЗ, СЗ)	22	22
лабораторные (ЛР)	11	11
Самостоятельная работа студентов (СРС)	53	53
Форма промежуточной аттестации в семестре	Зачет	0

Курсовая работа (курсовой проект) (КР, КП)	КП	

2. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Индекс компетенции	Содержание компетенции
ПК-3	Способность оценивать технические возможности и вырабатывать рекомендации по построению телекоммуникационных систем и сетей, их элементов и устройств
ПК-6	Способность применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду
ПК-7	Способность осуществлять рациональный выбор средств обеспечения информационной безопасности телекоммуникационных систем с учетом предъявляемых к ним требований качества обслуживания и качества функционирования
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

Планируемые результаты обучения по дисциплине для последовательного достижения уровней сформированности компетенций

Результат обучения	
Знать	Пороговый: • роль и место информационной безопасности в системе национальной безопасности страны; • угрозы информационной безопасности государства, организации, гражданина; • современные подходы к построению систем защиты информации; • компьютерную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности;

	Стандартный:
	Эталонный:
Уметь	Пороговый: • выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; • пользоваться современной научно-технической информацией по исследуемым проблемам и задачам;
	Стандартный:
	Эталонный:
Владеть	Пороговый: - навыками расчета и выбора основных параметров аппаратуры беспроводной связи, исходя из требований к качеству канала; - навыками эксплуатации оборудования беспроводных сетей; - навыками выбора оборудования и программного обеспечения для построения защищенных беспроводных сетей связи; - навыками интеграции беспроводных сетей связи в сетевую инфраструктуру предприятия, учитывая все аспекты обеспечения ее безопасности; - принципами мониторинга беспроводных сетей.
	Стандартный:
	Эталонный:

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	Организационные и физические защитные меры	14	2	6	0	6
	2	Специальные защитные меры систем ИТ	11	3	0	2	6
2	3	Обычно применяемые защитные меры	15	2	6	0	7
	4	Специальные защитные меры систем ИТ	12	3	0	2	7

3	5	Оценка проблем безопасности	12	3	0	2	7
	6	Защитные меры для обеспечения конфиденциальности	19	3	6	3	7
4	7	Идентификация типа системы ИТ	16	3	4	2	7
	8	Идентификация физических условий и условий окружающей среды	9	3	0	0	6
Итого			108	22	22	11	53

3.2. Лекционные занятия

Очная форма

Модуль	Номер раздела	Содержание лекционных занятий
1	1	Данная категория защитных мер содержит все защитные меры, имеющие отношение к управлению безопасностью ИТ, планированию деятельности, распределению полномочий и ответственности по этим процессам, а также все другие необходимые действия. Эти защитные меры описаны в ИСО/МЭК 13335-1 и 3* 9 ГОСТ Р ИСО/МЭК ТО 13335-4—2007 ИСО/МЭК ТО 13335-3. Целью этих защитных мер является достижение необходимого уровня безопасности организации
	2	Идентификация является средством, с помощью которого пользователь представляет заявленный идентификатор в систему. Аутентификация является средством валидации действительности этого заявления. Ниже приведены примеры достижения идентификации и аутентификации
2	3	Обычно применяются следующие категории защитных мер: - политика и управление безопасностью ИТ (см. 8.1.1); - проверка соответствия безопасности установленным требованиям (см. 8.1.2); - обработка инцидента (см. 8.1.3); - персонал (см. 8.1.4); - эксплуатационные вопросы (см. 8.1.5); - планирование непрерывности бизнеса (см. 8.1.6);
	4	меры для каждого типа компонента системы. Алгоритм выбора специальных защитных мер системы ИТ приведен в качестве примера в таблице 9.2. В этом примере знак «·» обозначает защитные меры, которые должны быть применены в нормальных условиях, а «(·)» — защитные меры, которые могут потре- боваться в особых случаях. Процесс выбора защитных мер должен быть продолжен путем рассмотрения их характеристик, представленных в 8.2. Дополнительная информация может быть получена из документов по базовой защите,

3	5	Для выбора соответствующих эффективных защитных мер организация должна исследовать и оце- нить проблемы безопасности, связанные с коммерческой деятельностью, которую обслуживает рассматри- ваемая система ИТ. После идентификации проблем безопасности и с учетом соответствующих угроз можно выбирать защитные меры согласно 10.2—10.5. Если подобная оценка покажет необходимость высокого уровня безопасности, то рекомендуется де- тальный подход к решению этой проблемы. Дополнительный материал можно найти в разделе 11. Проблемы безопасности могут включать в себя потерю: - конфиденциальности; - целостности; - доступности; - подотчетности; - аутентичности; - достоверности
	6	В данном разделе перечислены защитные меры от предполагаемых угроз, связанных с нарушением конфиденциальности. Кроме того, приведены соответствующие ссылки на защитные меры, в соответствии с разделом 8. Если эти защитные меры подходят при выборе защитных мер, то следует принять во внима- ние тип и характеристики системы ИТ. Большинство защитных мер, перечисленных в 8.1, обеспечивают более общую защиту, т. е. направ- лены на ряд угроз, и предоставляют защиту путем поддержки общего эффективного менеджмента безо- пасности ИТ. Настоящий стандарт не содержит подробного перечисления защитных мер, но их действие не должно быть недооценено и они должны быть реализованы для общей эффективной безопасности.
4	7	Для оценки существующей или планируемой системы ИТ организация должна сравнить рассматри- ваемую систему ИТ с перечисленными ниже компонентами. Организация должна идентифицировать ком- поненты, представляющие данную систему. Защитные меры для каждого из перечисленных компонентов представлены в разделе 9. К ним относятся: - автономная рабочая станция; - рабочая станция (клиент без ресурсов коллективного пользования), подсоединенная к сети; - сервер или рабочая станция с ресурсами коллективного пользования, подсоединенные к сети.
	8	Оценка окружающей среды включает в себя идентификацию физической инфраструктуры, поддержи- вающей существующую или планируемую систему ИТ и защитные меры к ней. Защитные меры должны соответствовать окружающей среде, поэтому подобная оценка является важным фактором для успешного выбора защитных мер. При рассмотрении физической инфраструктуры организация должна изучить окру- жающую среду и специальные обстоятельства, которые необходимо учесть.

3.3. Практические (семинарские) занятия

Очная форма

Модуль	Номер раздела	Содержание практических(семинарских) занятий
1	1	Данная категория защитных мер содержит все защитные меры, имеющие отношение к управлению безопасностью ИТ, планированию деятельности, распределению полномочий и ответственности по этим процессам, а также все другие необходимые действия. Эти защитные меры описаны в ИСО/МЭК 13335-1 и 3* 9 ГОСТ Р ИСО/МЭК ТО 13335-4—2007 ИСО/МЭК ТО 13335-3. Целью этих защитных мер является достижение необходимого уровня безопасности организации
2	3	Обычно применяются следующие категории защитных мер: - политика и управление безопасностью ИТ (см. 8.1.1); - проверка соответствия безопасности установленным требованиям (см. 8.1.2); - обработка инцидента (см. 8.1.3); - персонал (см. 8.1.4); - эксплуатационные вопросы (см. 8.1.5); - планирование непрерывности бизнеса (см. 8.1.6);
3	6	В данном разделе перечислены защитные меры от предполагаемых угроз, связанных с нарушением конфиденциальности. Кроме того, приведены соответствующие ссылки на защитные меры, в соответствии с разделом 8. Если эти защитные меры подходят при выборе защитных мер, то следует принять во внима- ние тип и характеристики системы ИТ. Большинство защитных мер, перечисленных в 8.1, обеспечивают более общую защиту, т. е. направ- лены на ряд угроз, и предоставляют защиту путем поддержки общего эффективного менеджмента безо- пасности ИТ. Настоящий стандарт не содержит подробного перечисления защитных мер, но их действие не должно быть недооценено и они должны быть реализованы для общей эффективной безопасности.
4	7	Для оценки существующей или планируемой системы ИТ организация должна сравнить рассматри- ваемую систему ИТ с перечисленными ниже компонентами. Организация должна идентифицировать ком- поненты, представляющие данную систему. Защитные меры для каждого из перечисленных компонентов представлены в разделе 9. К ним относятся: - автономная рабочая станция; - рабочая станция (клиент без ресурсов коллективного пользования), подсоединенная к сети; - сервер или рабочая станция с ресурсами коллективного пользования, подсоединенные к сети.

3.4. Лабораторные занятия

Очная форма

Модуль	Номер раздела	Содержание лабораторных занятий

1	2	Идентификация является средством, с помощью которого пользователь представляет заявленный идентификатор в систему. Аутентификация является средством валидации действительности этого заявления. Ниже приведены примеры достижения идентификации и аутентификации
2	4	меры для каждого типа компонента системы. Алгоритм выбора специальных защитных мер системы ИТ приведен в качестве примера в таблице 9.2. В этом примере знак «·» обозначает защитные меры, которые должны быть применены в нормальных условиях, а «(·)» — защитные меры, которые могут потре- боваться в особых случаях. Процесс выбора защитных мер должен быть продолжен путем рассмотрения их характеристик, представленных в 8.2. Дополнительная информация может быть получена из документов по базовой защите,
3	5	Для выбора соответствующих эффективных защитных мер организация должна исследовать и оце- нить проблемы безопасности, связанные с коммерческой деятельностью, которую обслуживает рассматри- ваемая система ИТ. После идентификации проблем безопасности и с учетом соответствующих угроз можно выбирать защитные меры согласно 10.2—10.5. Если подобная оценка покажет необходимость высокого уровня безопасности, то рекомендуется де- тальный подход к решению этой проблемы. Дополнительный материал можно найти в разделе 11. Проблемы безопасности могут включать в себя потерю: - конфиденциальности; - целостности; - доступности; - подотчетности; - аутентичности; - достоверности
	6	В данном разделе перечислены защитные меры от предполагаемых угроз, связанных с нарушением конфиденциальности. Кроме того, приведены соответствующие ссылки на защитные меры, в соответствии с разделом 8. Если эти защитные меры подходят при выборе защитных мер, то следует принять во внима- ние тип и характеристики системы ИТ. Большинство защитных мер, перечисленных в 8.1, обеспечивают более общую защиту, т. е. направ- лены на ряд угроз, и предоставляют защиту путем поддержки общего эффективного менеджмента безо- пасности ИТ. Настоящий стандарт не содержит подробного перечисления защитных мер, но их действие не должно быть недооценено и они должны быть реализованы для общей эффективной безопасности.

4	7	Для оценки существующей или планируемой системы ИТ организация должна сравнить рассматри- ваемую систему ИТ с перечисленными ниже компонентами. Организация должна идентифицировать ком- поненты, представляющие данную систему. Защитные меры для каждого из перечисленных компонентов представлены в разделе 9. К ним относятся: - автономная рабочая станция; - рабочая станция (клиент без ресурсов коллективного пользования), подсоединенная к сети; - сервер или рабочая станция с ресурсами коллективного пользования, подсоединенные к сети.

3.5. Организация самостоятельной работы

Очная форма

Модуль	Номер раздела	Содержание материала выносимого на самостоятельное изучение	Виды самостоятельной работы
1	1	защитные меры, описанные в ИСО/МЭК 13335-1	Реферат и выступление с докладом
2	3	категории защитных мер	Подготовка электронной презентации и ее представление
3	5	эффективные защитные меры	Реферат и выступление с докладом
3	6	защитные меры от предполагаемых угроз, связанных с нарушением конфиденциальности	Реферат и выступление с докладом
4	8	Оценка окружающей среды	Подготовка электронной презентации и ее представление

4. Интерактивные формы образовательных технологий

Модуль	Номер раздела	Вид учебных занятий	Образовательные технологии	Количество часов
1	1	ЛК	Физическая демонстрация с использованием презентации	2
2	3	ПР	Работа с электронными образовательными ресурсами	6
3	5	ЛК	Технологии проблемного обучения	3
4	8	ЛК	Физическая демонстрация с использованием презентации	3

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

Фонд оценочных средств

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Основная литература

6.1.1. Печатные издания

1.Клейменов С.А. Администрирование в информационных системах: учеб.пособие для студ.высш.учеб.заведений/С.А. Клейменов, В.П.Мельников, А.М. Петраков; под ред.В.П. Мельникова.-М.:Издательский центр «Академия», 2008.-272 с.
2. Современные телекоммуникации. Технологии и экономика / под ред. С.А. Довгого. - Москва : Эко-Трендз, 2003. - 320 с. - (Технологии электронных коммуникаций). - ISBN 5-88405-051-8 : 135-00.
3.Партыка Татьяна Леонидовна.
Информационная безопасность : учеб. пособие. - 5-е изд., перераб. и доп. - Москва : ФОРУМ, 2012. - 432 с. : ил. - (Профессиональное образование). - ISBN 978-5-91134-627-0 : 339-90.

6.1.2. Издания из ЭБС

1. Советов Борис Яковлевич.
Информационные технологии : Учебник / Советов Б.Я., Цехановский В.В. - 7-е изд. - Электрон. дан. - М : Издательство Юрайт, 2018. - 327. - (Профессиональное образование). - 7-е издание. - ISBN 978-5-534-06399-8 : 789.00.
2. Битнер В.И.
Сети нового поколения - NGN : Рекомендовано УМО по образованию в области телекоммуникаций в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению 210400 - "Телекоммуникации" / Битнер В.И.; Михайлова Ц.Ц. - Moscow : Горячая линия - Телеком, 2011. - . - Сети нового поколения - NGN [Электронный ресурс] : Учебное пособие для вузов / Битнер В.И., Михайлова Ц.Ц. - М. : Горячая линия - Телеком, 2011. - http://www.studentlibrary.ru/book/ISBN9785991201490.html. - ISBN 978-5-9912-0149-0

6.2. Дополнительная литература

6.2.1. Печатные издания

1. Гохберг Геннадий Соломонович.
Информационные технологии : учебник. - 4-е изд, стер. - Москва : Академия, 2008. - 208 с. : ил. - (Среднее профессиональное образование). - ISBN 978-5-7695-5474-2 : 213-22.
2. Битнер Владимир Иванович.
Нормирование качества телекоммуникационных услуг : учеб. пособие. - Москва : Горячая линия-Телеком, 2004. - 312с. : ил. - ISBN 5-93517-173-2 : 154-00.
3. Уткин Владимир Борисович.
Информационные технологии управления : учебник. - Москва : Академия, 2008. - 400 с. - (Высшее профессиональное образование). - ISBN 978-5-7695-3965-7 : 484-00.

6.2.2. Издания из ЭБС

6.3. Базы данных, информационно-справочные и поисковые системы

1 . Информационная система «Единое окно доступа к образовательным ресурсам» (http://window.edu.ru/).
2. Научная Электронная Библиотека http://www.e-library.ru.
3 . Электронные версии учебников, пособий, методических разработок, указаний и

рекомендаций по всем видам учебной работы, предусмотренных вузовской рабочей программой, находящиеся в свободном доступе для студентов, обучающихся в вузе

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, д.1, корп. 1, ауд. 08-206
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.
Наборы демонстрационного оборудования и учебно-наглядных пособий по дисциплинам, переносной мультимедийный к-т в составе: экран на треноге, мультимедиапроектор, ноутбук.
MS Office Standart 2013 (договор № 223-798 от 30.12.2014 г., срок действия - бессрочно; договор № 223-799 от 30.12.2014г., срок действия - бессрочно) Mozilla Firefox Право использования программного обеспечения предоставляется по MPL лицензии (https://www.mozilla.org/ru/firefox/) (срок действия - право использования программного обеспечения действует до изменения политики правообладателя) АИБС «МегаПро» (договор № 13215/223П/15-569 от 18.12.2015 г.)

9. Методические рекомендации по организации изучения дисциплины

Лекции являются основным источником теоретического материала по дисциплине. Посещение и конспектирование лекций является обязательной составляющей успешного освоения дисциплины обучающимися.
Для эффективного освоения материала дисциплины 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
Отчет студента по работе должен быть индивидуальным, составленным по установленной форме, и содержать следующие разделы: наименование работы; цель работы; индивидуальное задание; применяемая аппаратура; ее 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 на вопросы для самоконтроля по 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.
На 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: Заведующий кафедрой ФиТС, Свешников Игорь Вадимович

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