

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.30.Криптографические методы защиты информации

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 изучения дисциплины является формирование у магистрантов общих представлений о содержании криптографических методов защиты информации и о подходах к оценке эффективности таких методов.

Задачи изучения дисциплины:

Задачи дисциплины: - дать представление об информационной безопасности, как сфере профессиональной деятельности; - раскрыть особенности криптографических методов защиты информации и содержание базовых понятий криптографии; - ознакомить с основными видами шифров; - ознакомить с современными стандартами криптографической защиты; - дать представление об атаках на криптографические системы.

1.2. Место дисциплины (модуля) в структуре ОП

Место дисциплины в структуре ООП бакалавриата Дисциплина «Криптографические методы защиты информации» входит в учебный план (раздел Б3. ДВ2) подготовки бакалавров по профессионально-образовательной программе направления «Математика и компьютерные науки» для профиля подготовки «Математический анализ и приложения» как дисциплина по выбору вариативной части профессионального цикла. Освоение криптографических методов защиты информации необходимо для профессиональной подготовки бакалавров. Для освоения дисциплины необходимо знание курсов: «Математический анализ», «Алгебра и теория чисел», «Численные методы». В результате изучения данной дисциплины студенты освоят непростые математические принципы организации криптографической защиты информации, передаваемой и обрабатываемой техническими средствами, что является неотъемлемой составляющей подготовки учащихся по направлению «Математика и компьютерные науки». Курс необходим для дисциплин компьютерной безопасности. 3. Компетенции обучающегося, формируемые в результате освоения дисциплины «Криптографические методы защиты информации» Выпускник должен обладать следующими общекультурными компетенциями компетенциями (ОК): способностью применять в научно-исследовательской и профессиональной деятельности базовые знания в области фундаментальной и прикладной математики и естественных наук (ОК-6); Выпускник должен обладать следующими профессиональными компетенциями (ПК): владением методом алгоритмического моделирования при анализе постановок математических задач (ПК-19); владением методами математического и алгоритмического моделирования при анализе и решении прикладных и инженерно-технических проблем (ПК-20). В результате освоения дисциплины «Криптографические методы защиты информации» обучающийся должен: Знать: основные термины и понятия криптографии, этапы развития криптографии; вид информации, подлежащей шифрованию; требования к шифрам и их основные характеристики; классификацию шифров; принципы расчета параметров типовых

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
	7 семестр	8 семестр	

Общая трудоемкость			216
Аудиторные занятия, в т.ч.	34	64	98
лекционные (ЛК)	17	32	49
практические (семинарские) (ПЗ, СЗ)	0	16	16
лабораторные (ЛР)	17	16	33
Самостоятельная работа студентов (СРС)	38	44	82
Форма промежуточной аттестации в семестре	Зачет	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-15	Способность проводить инструментальный мониторинг защищенности телекоммуникационных систем, обеспечения требуемого качества обслуживания

Планируемые результаты обучения по дисциплине для последовательного достижения уровней сформированности компетенций

Результат обучения	
Знать	Пороговый:
	Стандартный:
	Эталонный:

Уметь	Пороговый: умение извлекать актуальную научно-техническую информацию из электронных библиотек, реферативных журналов
	Стандартный: способность к творческому применению, развитию и реализации математически сложных алгоритмов в современных программных комплексах
	Эталонный: способность работать в междисциплинарной команде
Владеть	Пороговый: владение методами математического и алгоритмического моделирования при анализе проблем естествознания
	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	Криптографические методы защиты	42	16	8	8	10
2	2	Электронный сертификат	0				
3	3	Криптопровайдеры	0				
4	4	Инфраструктура открытых ключей	0				
5	5	Аппаратные средства аутентификации	0				
Итого			42	16	8	8	10

3.2. Лекционные занятия

Очная форма

Модуль	Номер раздела	Содержание лекционных занятий
1	1	
2	2	Сертификат X.509 Основной контекст сертификата Расширения сертификатов Классы сертификатов Закрытые ключи, расположенные в профиле пользователя
3	3	КриптоАРМ Рутокен КриптоПро CSP
4	4	Архитектура Windwos 2003 Certificate Services Проблема отзыва сертификатов Протокол OCSP Служба сертификации в Windwos 2003 R2 Стандарты и области PKI
5	5	Аппаратные средства аутентификации с использованием пароля Аутентификация с использованием смарт карт и PKI Системы одноразовых паролей SecurID

3.3. Практические (семинарские) занятия

Очная форма

Модуль	Номер раздела	Содержание практических(семинарских) занятий
2	2	Установка eToken PKI client инициализация e Token PRO Java Получение сертификата eToken

3	3	Установка Рутокен Получение сертификата на рутокен
4	4	Установка СКЗИ КriptoПро Получение сертификатов с использованием СКЗИ КriptoПро

3.4. Лабораторные занятия

Очная форма

Модуль	Номер раздела	Содержание лабораторных занятий
4	4	Создание корневого центра сертификации
5	5	Настройка входа по смарт карте с сертификатом X 509 Настройка двухфакторной аутентификации без сертификатов X 509 с использованием eToken TMS Настройка двухфакторной аутентификации с сертификатов X 509 с использованием eToken TMS

3.5. Организация самостоятельной работы

Очная форма

Модуль	Номер раздела	Содержание материала выносимого на самостоятельное изучение	Виды самостоятельной работы
1	1	Криптографические методы защиты	составление конспекта, работа с литературой
2	2	Электронный сертификат	составление конспекта, работа с литературой
3	3	Криптопровайдеры	составление конспекта, работа с литературой
4	4	Инфраструктура открытых ключей	составление конспекта, работа с литературой
5	5	Аппаратные средства аутентификации	составление конспекта, работа с литературой

4. Интерактивные формы образовательных технологий

Модуль	Номер раздела	Вид учебных занятий	Образовательные технологии	Количество часов
1	1	ЛК	интерактивные лекции с использованием мультимедиа; разбор конкретных ситуаций (ситуационные задачи);	6

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. 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.
2. Мельников, Владимир Павлович. Информационная безопасность и защита информации : учеб. пособие для студ. высш. учеб. заведений / под ред. С.А. Клейменова. - 5-е изд., стер. - Москва : Академия, 2011. - 336 с. - ISBN 978-5-7695-7738-3 : 398-20.
3. Информационная безопасность и защита информации : учеб. пособие. - Старый Оскол : ТНТ, 2010. - 384 с. - ISBN 978-5-94178-216-1 : 385-00.

6.1.2. Издания из ЭБС

1. Бабенко, Людмила Климентьевна. Криптографическая защита информации: симметричное шифрование : Учебное пособие / Бабенко Л.К., Ищукова Е.А. - М. : Издательство Юрайт, 2017. - 220. - (Университеты России). - ISBN 978-5-9916-9244-1 : 72.07.
2. Щеглов, Андрей Юрьевич. Защита информации: основы теории : Учебник / Щеглов А.Ю., Щеглов К.А. - М. : Издательство Юрайт, 2017. - 309. - (Бакалавр и магистр. Академический курс). - ISBN 978-5-534-04732-5 : 1000.00 .
3. Внуков, Андрей Анатольевич. Защита информации : Учебное пособие / Внуков А.А. - 2-е изд. - М. : Издательство Юрайт, 2017. - 261. - (Бакалавр и магистр. Академический курс). - ISBN 978-5-534-01678-9 : 78.62 .

6.2. Дополнительная литература

6.2.1. 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. Чеботарева, Анна Александровна. Информационное право : учеб. пособие. - Чита : ЗабГУ, 2012. - 202 с. - ISBN 978-5-9293-0784-3 : 143-00.

6.2.2. Издания из ЭБС

1. Лось, Алексей Борисович. Криптографические методы защиты информации : Учебник /

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 "МераПро".

Программное обеспечение специального назначения:

8. Материально-техническое обеспечение дисциплины

672000, г. Чита, ул. Кастринская, д. 1. 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, д. 1. 08-310а. Лаборатория программно-аппаратных средств обеспечения защиты информации. Лаборатория технической 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 , APM VipNet клиент (12 лицензий) учебная защищенная сеть.

672000, г. Чита, ул. Кастринская, д. 1. 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 MC 240 Зав.№403.

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 составлении 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; и т.о 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 умения 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: Свешников Игорь Вадимович, зав.кафедрой

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