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

Энергетический факультет

Кафедра Информатики вычислительной техники и прикладной математики

УТВЕРЖДАЮ:

Декан факультета

Мирошников С.Ф.

«____»_____20____г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.Б.18.Защита информации

на 144 часа(ов), 4 зачетных(ые) единиц(ы)

для направления подготовки (специальности) 09.03.01 – Информатика и вычислительная техника

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

Профиль – Программное обеспечение вычислительной техники и автоматизированных систем (для набора 2013, 2014)

Форма обучения очная, заочная

1. Организационно-методический раздел

1.1 Цель и задачи дисциплины (модуля)

Цель изучения дисциплины:

Целью изучения дисциплины является получение студентами фундаментальных знаний в области обеспечения информационной безопасности информационных ресурсов, автоматизированных систем и вычислительных сетей.

Задачи изучения дисциплины:

В результате изучения дисциплины студенты должны уметь:
- проводить оценку рисков нарушения информационной безопасности;
- разрабатывать политики информационной безопасности;
- использовать специальные технические средства для защиты информации;
- использовать криптографические средства для защиты конфиденциальной информации.

1.2. Место дисциплины (модуля) в структуре ОП

Дисциплина «Защита информации» является специализированной. Теоретические и практические навыки, полученные при изучении данной дисциплины, будут востребованы при организации системы информационной безопасности на предприятии. Для успешного освоения дисциплины «Защита информации» студент должен иметь базовую подготовку по дисциплинам «Сети и телекоммуникации», «Операционные системы» согласно учебного плана направления 09.03.01. Дисциплина «Защита информации» входит в состав Блока 1 базовую часть.

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
	8 семестр	
Общая трудоемкость		144
Аудиторные занятия, в т.ч.	54	54
лекционные (ЛК)	36	36
практические (семинарские) (ПЗ, СЗ)	0	0
лабораторные (ЛР)	18	18
Самостоятельная работа студентов (СРС)	54	54
Форма промежуточной аттестации в семестре	Экзамен	36

Курсовая работа (курсовой проект) (КР, КП)		

Заочная форма

Виды занятий	Распределение по семестрам	Всего часов
	9 семестр	
Общая трудоемкость		144
Аудиторные занятия, в т.ч.	14	14
лекционные (ЛК)	6	6
практические (семинарские) (ПЗ, СЗ)	0	0
лабораторные (ЛР)	8	8
Самостоятельная работа студентов (СРС)	94	94
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
ОК-2	Способность анализировать основные этапы и закономерности исторического развития общества для формирования гражданской позиции
ОПК-5	Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ПК-2	Способность разрабатывать компоненты аппаратно-программных комплексов и баз данных, используя современные инструментальные средства и технологии программирования

Планируемые результаты обучения по дисциплине для последовательного достижения уровней сформированности компетенций

Результат обучения	
Знать	Пороговый: 1) Основные стандарты информационной безопасности 2) Правовые основы защиты информации. 3) Основные угрозы безопасности информации. 4) Классификацию алгоритмов шифрования
	Стандартный: 1) Возможности технических средств для защиты информации. 2) Методы оценки рисков и построения модели угроз. 3) Основные криптографические модели
	Эталонный: 1) Алгоритмы .построения комплексной системы безопасности 2) Алгоритмы шифрования
Уметь	Пороговый: 1) Разрабатывать политику безопасности. 2) Настраивать технические средства защиты информации.
	Стандартный: 1) Разрабатывать частные модели угроз 2) Администрировать удостоверяющий центр
	Эталонный: 1) Разрабатывать криптографические средства защиты
Владеть	Пороговый: 1) Инструментами операционной системы в целях защиты информации.
	Стандартный: 1) Инструментами для организации безопасности вычислительных сетей 2) Ключевой инфраструктурой предприятия.
	Эталонный: 1) Алгоритмами организации комплексной безопасности предприятия на основе анализа рисков.

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	Основные понятия и определения. Правовые аспекты. Оценка рисков.	30	12	0	4	14
2	2	Криптография и криптоанализ.	48	16	0	8	24
3	3	Организация комплексной системы информационной безопасности	30	8	0	6	16
Итого			108	36	0	18	54

Заочная форма

Модуль	Номер раздела	Наименование раздела	Всего часов	Аудиторные занятия			СРС
				ЛК	ПЗ(СЗ)	ЛР	
1	1	Основные понятия и определения. Правовые аспекты. Оценка рисков.	28	2	0	2	24
2	2	Криптография и криптоанализ.	46	2	0	4	40
3	3	Организация комплексной системы информационной безопасности	34	2	0	2	30
Итого			108	6	0	8	94

3.2. Лекционные занятия

Очная форма

Модуль	Номер раздела	Содержание лекционных занятий
1	1	Основные понятия и определения. Источники, риски и формы атак на информацию. Правовые аспекты безопасности информационных технологий. Стандарты безопасности. Оценка рисков нарушения информационной безопасности. Модели угроз. Политика информационной безопасности.
2	2	Криптография и криптоанализ. Криптографические модели. Алгоритмы шифрования. Алгоритмы аутентификации пользователей. Криптографические методы. Симметричные криптографические системы. Асимметричные криптографиические системы. Электронно-цифровая подпись. Функционирование удостоверяющего центра.

3	3	Безопасность современных сетевых технологий. Защита информации в сетях. Комплексная система информационной безопасности предприятия. Особенности защиты информационных си-стем персональных данных.

Заочная форма

Модуль	Номер раздела	Содержание лекционных занятий
1	1	Основные понятия и определения. Источники, риски и формы атак на информацию. Правовые аспекты безопасности информационных технологий. Стандарты безопасности. Оценка рисков нарушения информационной безопасности. Модели угроз. Политика информационной безопасности.
2	2	Криптография и криптоанализ. Криптографические модели. Алгоритмы шифрования. Алгоритмы аутентификации пользователей. Криптографические методы. Симметричные криптографические системы. Асимметричные криптографиические системы. Электронно-цифровая подпись. Функционирование удостоверяющего центра.
3	3	Безопасность современных сетевых технологий. Защита информации в сетях. Комплексная система информационной безопасности предприятия. Особенности защиты информационных си-стем персональных данных.

3.3. Практические (семинарские) занятия

3.4. Лабораторные занятия

Очная форма

Модуль	Номер раздела	Содержание лабораторных занятий

1	1	Исследование информационных ресурсов, оценка рисков, построение модели угроз. Разработка политики информационной безопасности
2	2	Исследование средств информационной безопасности операционных систем. Установка и настройка Крипто-про. Работа с закрытыми и открытыми ключами. Установка и настройка удостоверяющего центра. Получение ЭЦП. Шифрование данных. Электронная подпись.
3	3	Настройка VPN-канала. Установка и настройка антивирусного программного обеспечения. Установка и настройка межсетевого экрана. Разработка политики защиты информационной системы персональных данных.

Заочная форма

Модуль	Номер раздела	Содержание лабораторных занятий
1	1	Исследование информационных ресурсов, оценка рисков, построение модели угроз. Разработка политики информационной безопасности
2	2	Исследование средств информационной безопасности операционных систем. Установка и настройка Крипто-про. Работа с закрытыми и открытыми ключами. Установка и настройка удостоверяющего центра. Получение ЭЦП. Шифрование данных. Электронная подпись.
3	3	Настройка VPN-канала. Установка и настройка антивирусного программного обеспечения. Установка и настройка межсетевого экрана. Разработка политики защиты информационной системы персональных данных.

3.5. Организация самостоятельной работы

Очная форма

Модуль	Номер раздела	Содержание материала выносимого на самостоятельное изучение	Виды самостоятельной работы

1	1	Основные понятия и определения. Источники, риски и формы атак на информацию. Правовые аспекты безопасности информационных технологий. Стандарты безопасности. Оценка рисков нарушения информационной безопасности. Модели угроз. Политика информационной безопасности.	работа с компьютерными моделями
2	2	Криптография и криптоанализ. Криптографические модели. Алгоритмы шифрования. Алгоритмы аутентификации пользователей. Криптографические методы. Симметричные криптографические системы. Асимметричные криптографиические системы. Электронно-цифровая подпись. Функционирование удостоверяющего центра.	работа с компьютерными моделями
3	3	Безопасность современных сетевых технологий. Защита информации в сетях. Комплексная система информационной безопасности предприятия. Особенности защиты информационных си-стем персональных данных.	работа с компьютерными моделями

Заочная форма

Модуль	Номер раздела	Содержание материала выносимого на самостоятельное изучение	Виды самостоятельной работы
1	1	Основные понятия и определения. Источники, риски и формы атак на информацию. Правовые аспекты безопасности информационных технологий. Стандарты безопасности. Оценка рисков нарушения информационной безопасности. Модели угроз. Политика информационной безопасности.	работа с компьютерными моделями
2	2	Криптография и криптоанализ. Криптографические модели. Алгоритмы шифрования. Алгоритмы аутентификации пользователей. Криптографические методы. Симметричные криптографические системы. Асимметричные криптографиические системы. Электронно-цифровая подпись. Функционирование удостоверяющего центра.	работа с компьютерными моделями
3	3	Безопасность современных сетевых технологий. Защита информации в сетях. Комплексная система информационной безопасности предприятия. Особенности защиты информационных си-стем персональных данных.	работа с компьютерными моделями

4. Интерактивные формы образовательных технологий

Модуль	Номер раздела	Вид учебных занятий	Образовательные технологии	Количество часов
1	1	лекции	лекции с использованием презентаций	12
1	1	лабораторные работы	информационные технологиий	4
2	2	лекции	лекции с использованием презентаций	16
2	2	лабораторные работы	информационные технологии	8
3	3	лекции	лекции с использованием презентаций	8
6	3	лабораторные работы	информационные технологии	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 Т.Л. Информационная безопасность: учеб. пособие / Т.Л. Партыка, И.И. Попов. – 5-е изд., перераб. и доп. – Москва: ФОРУМ, 2012. – 432с.
2. Мельников В.П. Информационная безопасность и защита информа-ции: учеб. пособие для студ. высш. учеб. заведений / В.П. Мельников, С.А. Клейменов, А.М.Петраков; под ред. С.А. Клейменова. – 5-е изд., стер. – Москва: Академия, 2011. – 336 с.
3. Громов Ю.Ю. Информационная безопасность и защита информации : учеб. пособие / Ю.Ю. Громов – Старый Оскол : ТНТ, 2010. - 384с.

6.1.2. Издания из ЭБС

1. Внуков А. А. Защита информации : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2017. — 261 с. — То же [Электронный ресурс]. – URL: www.biblio-online.ru/book/73BEF88E-FC6D-494A-821C-D213E1A984E1.
2. Щеглов А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — М. : Издательство Юрайт, 2017. — 309 с. — То же [Электронный ресурс]. – URL: https://www.biblio-online.ru/book/9CD7BE3A-F9DC-4F6D-8EC6-6A90CB9A4E0E.

6.2. Дополнительная литература

6.2.1. Печатные издания

1. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: учеб. пособие / П.Б.Хорев. – 4-е изд., стер. – Москва: Академия, 2008. – 256с.
2. Никонов Е. А. Сети и телекоммуникации: учеб. пособие / Е.А. Никонов, Д.А. Семигузов. – Чита: ЗабГУ, 2013. – 135 с.
3. Чеботарева А.А. Информационное право : учеб. пособие / А.А. Чеботарева. - Чита : ЗабГУ, 2012. - 202 с

6.2.2. Издания из ЭБС

9. Лось, А. Б. Криптографические методы защиты информации : учебник для академического бакалавриата / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — М. : Издательство Юрайт, 2017. — 473 с. — То же [Электронный ресурс] – URL: www.biblio-online.ru/book/27397D56-C8A1-4970-9F39-28E7FA40632A.
10. Полякова Т. А. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под ред. Т. А. Поляковой, А. А. Стрельцова. — М. : Издательство Юрайт, 2017. — 325 с. — То же [Электронный ресурс] – URL: https://www.biblio-online.ru/book/D056DF3D-E22B-4A93-8B66-EBBAEF354847.

6.3. Базы данных, информационно-справочные и поисковые системы

1. https://www.biblio-online.ru/ Электронно-библиотечная система «Юрайт».
2. http://www.studentlibrary.ru/ Электронно-библиотечная система «Консультант студента».
3. http://www.edu.ru Федеральный портал «Российское образование».
4. http://window.edu.ru Информационная система «Единое окно доступа к образовательным ресурсам» предоставляет свободный доступ к каталогу образовательных Интернет-ресурсов и полнотекстовой электронной учебно-методической библиотеке для общего и профессионального образования.
5. http://studentam.net/ Электронная библиотека учебников.
6. http://da8.boom.ru Каталог ссылок на научную литературу в Сети.

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: Visual Studio Community

8. Материально-техническое обеспечение дисциплины

Компьютерный класс. Учебная аудитория 03-400 для проведения занятий лекционного типа, занятий семинарского типа, курсового и дипломного проектирования (выполнения курсовых и дипломных работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, самостоятельной работы, адрес аудитории: 672039, Забайкальский край, г. Чита, ул. Баргузинская, 49, корп. 1
Специализированная учебная мебель, доска магнитно-маркерная, учебно-наглядные пособия (переносные), мультимедийный проектор (переносной), ноутбук (переносной), 15 компьютеров с подключением к сети «Интернет» и доступом в электронную информационно-образовательную среду организации

9. Методические рекомендации по организации изучения дисциплины

Методические рекомендации к лекционным занятиям.
В ходе лекционных занятий необходимо вести конспектирование учебного материала.
Методические рекомендации по подготовке к лабораторным работам.
Целью проведения лабораторных занятий является углубление и закрепление на практике теоретических знаний, полученных на лекциях и в процессе самостоятельного изучения учебного материала, а, следовательно, формирование у них определенных умений и навыков. В ходе подготовки к лабораторному занятию необходимо прочитать конспект лекции, изучить основную литературу, ознакомиться с дополнительной литературой, дорабатывая свой конспект лекции, делая в нем соответствующие записи из литературы. Желательно при подготовке к лабораторным занятиям по дисциплине одновременно использовать несколько источников, раскрывающих заданные вопросы. В ходе лабораторного занятия требуется выполнить выданные преподавателем задачи, с

учетом рекомендаций преподавателя.
Методические рекомендации по организации самостоятельной работы. Самостоятельная работа требуется для получения новых знаний и закреплению и углублению имеющихся. знаний, формированию профессиональных навыков и умений. Самостоятельная работа выполняет ряд функций: информационно-обучающую, ориентирующую, исследовательскую. Это и позволяет сформировать нужные компетенции в ходе изучения дисциплины. В ходе самостоятельного обучения требуется ознакомление с рекомендуемой литературой, представленной библиотекой ВУЗа. Также возможно углубление знаний за счет источников, расположенных в сети Интернет. Результаты самостоятельной работы оцениваются по рассмотрению выполняемых заданий, вынесенных преподавателем на самостоятельную работу

Разработчик/группа разработчиков: Семигузов Д.А. - доцент ИВТиПМ

Рассмотрена на заседании кафедры
(протокол от 01.09.2017 г. № 1)