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

Энергетический факультет

Батухтин Андрей Геннадьевич

«____»_____20____ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.О.20 Защита информации
на 180 часа(ов), 5 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 – Вычислительные машины, комплексы, системы и сети (для набора 2022)
Форма обучения: Очная

1. Организационно-методический раздел

1.1 Цели и задачи дисциплины (модуля)

Цель изучения дисциплины:

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

Задачи изучения дисциплины:

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.

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

Общая трудоемкость дисциплины (модуля) составляет 5 зачетных(ые) единиц(ы), 180 часов.

Виды занятий	Семестр 7	Семестр 8	Всего часов
Общая трудоемкость			180
Аудиторные занятия, в т.ч.	34	36	70
Лекционные (ЛК)	17	18	35
Практические (семинарские) (ПЗ, СЗ)	0	0	0
Лабораторные (ЛР)	17	18	35
Самостоятельная работа студентов (СРС)	38	36	74

Форма промежуточной аттестации в семестре	Зачет	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
ОПК-3	ОПК-3.1.Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Знать: современные информационные технологии и программные средства, в том числе отечественного производства, используемые для разработки и эксплуатации web-приложений, при решении задач профессиональной деятельности.
ОПК-3	ОПК-3.2. Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
ОПК-3	ОПК-3.3. Иметь навыки: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	Владеть: навыками применения современных информационных технологий и программные средства, в том числе отечественного производства, используемые для разработки и эксплуатации web-приложений, при решении задач профессиональной деятельности.

ОПК-8	ОПК-8.1. Знать: основные языки программирования и работы с базами данных, операционные системы и оболочки, современные программные среды разработки информационных систем и технологий.	Знать: основные языки программирования, современные программные среды разработки и отладки программ, способы взаимодействия с операционными системами.
ОПК-8	ОПК-8.2. Уметь: применять языки программирования и работы с базами данных, современные программные среды разработки информационных систем и технологий для автоматизации бизнес-процессов, решения прикладных задач различных классов, ведения баз данных и информационных хранилищ.	Уметь: применять языки программирования и современные программные среды разработки программ для решения прикладных задач различного класса, связанных с автоматизацией бизнес-процессов и ведением информационных хранилищ данных.
ОПК-8	ОПК-8.3. Иметь навыки: программирования, отладки и тестирования прототипов программно-технических комплексов задач.	Владеть: навыками программирования,отладки и тестирования прототипов различных информационных комплексов.
ПК-9	ПК-9.1 Знать: принципы организации целостности и доступности БД (атомарность, структурированность)	Знать: принципы организации целостности и доступности БД автоматизированных систем
ПК-9	ПК-9.2. Уметь: реализовывать криптографические алгоритмы защиты данных.	Уметь: реализовывать криптографические алгоритмы защиты данных.
ПК-9	ПК-9.3 Иметь навыки: безопасного администрирования СУБД	Владеть: Навыками безопасного администрирования СУБД на уровне групповых политик домена
ПК-13	ПК-13.1. Знать: методы и средства аутентификации и авторизации	Знать: методы и средства аутентификации и авторизации
ПК-13	ПК-13.2. Уметь: разворачивать программные и аппаратные средства криптографической защиты	Уметь: разворачивать программные и аппаратные средства криптографической защиты
ПК-13	ПК-13.3. Иметь навыки: безопасного администрирования вычислительной сети и сетевых узлов	Владеть: Навыками безопасного администрирования вычислительной сети и сетевых узлов на основе групповых политик домена

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	Основные понятия и определения. Правовые аспекты. Оценка рисков.	Основные понятия и определения. Источники, риски и формы атак на информацию. Правовые аспекты безопасности информационных технологий. Стандарты безопасности. Оценка рисков нарушения информационной безопасности. Модели нарушителя. Модели угроз.	20	4	0	4	12
2	2.1	Основные меры обеспечения безопасности информации.	Виды мер обеспечения безопасности информации. Организационные меры. Организационные меры. Технические и технологические меры.	24	6	0	6	12
3	3.1	Обнаружение атак.	Механизмы идентификации, аутентификации, авторизации. Криптографические средства. Контроль целостности. Резервирование и резервное копирование. Фильтрация трафика, обнаружение атак и вредоносного кода,	28	7	0	7	14

			обнаружение уязвимостей.					
4	4.1	Организация комплексной системы информационной безопасности	Безопасность современных сетевых технологий. Защита информации в сетях. Комплексная система информационной безопасности предприятия. Особенности защиты информационных систем персональных данных и критической информационной инфраструктуры..	28	6	0	6	16
5	5.1	Криптография и криптоанализ.	Криптография и криптоанализ. Криптографические модели. Алгоритмы шифрования. Алгоритмы аутентификации пользователей. Криптографические методы. Симметричные криптографические системы. Асимметричные криптографиические системы. Электронно-цифровая подпись. Функционирование удостоверяющего центра.	44	12	0	12	20
Итого				144	35	0	35	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	Основные понятия и определения.	Основные понятия и определения. Источники, риски и формы атак на информацию. Правовые аспекты	4

		Источники, риски и формы атак на информацию. Правовые аспекты безопасности информационных технологий. Стандарты безопасности. Оценка рисков нарушения информационной безопасности. Модели нарушителя. Модели угроз.	безопасности информационных технологий. Стандарты безопасности. Оценка рисков нарушения информационной безопасности. Модели нарушителя. Модели угроз.	
2	2.1	Виды мер обеспечения безопасности информации. Организационные меры. Организационные меры. Технические и технологические меры.	Виды мер обеспечения безопасности информации. Организационные меры. Организационные меры. Технические и технологические меры.	6
3	3.1	Механизмы идентификации, аутентификации, авторизации. Криптографические средства. Контроль целостности. Резервирование и резервное копирование. Фильтрация трафика, обнаружение	Механизмы идентификации, аутентификации, авторизации. Криптографические средства. Контроль целостности. Резервирование и резервное копирование. Фильтрация трафика, обнаружение атак и вредоносного кода, обнаружение уязвимостей.	7

		атак и вредоносного кода, обнаружение уязвимостей.		
4	4.1	Безопасность современных сетевых технологий. Защита информации в сетях. Комплексная система информационной безопасности предприятия. Особенности защиты информационных систем персональных данных и критической информационной инфраструктуры.	Безопасность современных сетевых технологий. Защита информации в сетях. Комплексная система информационной безопасности предприятия. Особенности защиты информационных систем персональных данных и критической информационной инфраструктуры.	6
5	5.1	Криптография и криптоанализ. Криптографические модели. Алгоритмы шифрования. Алгоритмы аутентификации пользователей. Криптографические методы. Симметричные криптографические системы. Асимметричные криптографиические системы. Элек	Криптография и криптоанализ. Криптографические модели. Алгоритмы шифрования. Алгоритмы аутентификации пользователей. Криптографические методы. Симметричные криптографические системы. Асимметричные криптографиические системы. Электронно-цифровая подпись. Функционирование удостоверяющего центра.	12

		тронно-цифровая подпись. Функционирование удостоверяющего центра.		

3.2.2. Практические занятия, содержание и объем в часах

Модуль	Номер раздела	Тема	Содержание	Трудоемкость (в часах)

3.2.3. Лабораторные занятия, содержание и объем в часах

Модуль	Номер раздела	Тема	Содержание	Трудоемкость (в часах)
1	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 нарушителя. Модели угроз.	Исследование информационных ресурсов, оценка рисков, построение модели угроз. Разработка политики информационной безопасности	4
2	2.1	Виды мер обеспечения безопасности информации. Организацион	Разработка организационно-распорядительных и нормативных документов	6

		ные меры. Организационные меры. Технические и технологические меры.		
3	3.1	Механизмы идентификации, аутентификации, авторизации. Криптографические средства. Контроль целостности. Резервирование и резервное копирование. Фильтрация трафика, обнаружение атак и вредоносного кода, обнаружение уязвимостей.	Исследование средств информационной безопасности операционных систем. Установка и настройка Крипто-про. Установка и настройка антивирусного программного обеспечения. Установка и настройка межсетевого экрана.	7
4	4.1	Безопасность современных сетевых технологий. Защита информации в сетях. Комплексная система информационной безопасности предприятия. Особенности защиты информационных систем персональных данных и критической информационной инфрастру	Настройка VPN-канала. установка и настройка систем обнаружения атак. Настройка доменных политик безопасности.	6

		ктуры.		
5	5.1	Криптография и криптоанализ. Криптографические модели. Алгоритмы шифрования. Алгоритмы аутентификации пользователей. Криптографические методы. Симметричные криптографические системы. Асимметричные криптографиические системы. Электронно-цифровая подпись. Функционирование удостоверяющего центра.	Разработка приложений, реализующих криптографические алгоритмы. Установка и настройка удостоверяющего центра	12

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	Основные понятия и определения. Источники, риски и формы атак на информацию. Правовые аспекты безопасности информационных технологий. Стандарты безопасности. Оценка рисков нарушения информационной безопасности. Модели нарушителя. Модели	Изучение литературы. Работа с компьютерными моделями. Решение задач. Разработка приложений.	12

		угроз.		
2	2.1	Разработка организационно-распорядительных и нормативных документов	Изучение литературы. Работа с компьютерными моделями. Решение задач. Разработка приложений.	12
3	3.1	Исследование средств информационной безопасности операционных систем. Установка и настройка Крипто-про. Установка и настройка антивирусного программного обеспечения. Установка и настройка межсетевого экрана.	Изучение литературы. Работа с компьютерными моделями. Решение задач. Разработка приложений.	14
4	4.1	Настройка VPN-канала. установка и настройка систем обнаружения атак. Настройка доменных политик безопасности.	Изучение литературы. Работа с компьютерными моделями. Решение задач. Разработка приложений.	16
5	5.1	Разработка приложений, реализующих криптографические алгоритмы. Установка и настройка удостоверяющего центра	Изучение литературы. Работа с компьютерными моделями. Решение задач. Разработка приложений.	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. 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.

5.1.2. 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.

5.2. Дополнительная литература

5.2.1. 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.

5.2.2. Издания из ЭБС

1. 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.
2. 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.

5.3. Базы данных, информационно-справочные и поисковые системы

Название	Ссылка
Электронно-библиотечная система «Юрайт».	https://www.biblio-online.ru/
Электронно-библиотечная система «Консультант студента».	http://www.studentlibrary.ru/

Электронно-библиотечная система «Издательство «Лань»».	https://e.lanbook.com/

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) JetBrain IntelliJ IDEA

2) JetBrain PyCharm

3) NetEmul

4) Python

5) Visual Studio Community

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 лабораторных занятий	
Учебные аудитории для промежуточной аттестации	
Учебные аудитории для проведения групповых и индивидуальных консультаций	Состав оборудования и технических средств обучения указан в паспорте аудитории, закрепленной расписанием по кафедре
Учебные аудитории для текущей аттестации	

8. Методические рекомендации по организации изучения дисциплины

В ходе лекционных занятий необходимо вести конспектирование учебного материала. 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.

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:
Анатолий Анатольевич Забелин

Типовая программа утверждена

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