МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Директор ИШЭ
_____Матвеев А.С.
«26» июня 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ПРИЕМ 2019 г.
ФОРМА ОБУЧЕНИЯ очно-заочная

Информационная безопасность и защита информации

Направление подготовки/ специальность	**09.04.03 Прикладная информатика**		
Образовательная программа (направленность (профиль))	**Информационные технологии в электроэнергетике**		
Специализация	Информационные технологии в электроэнергетике		
Уровень образования	высшее образование - магистратура		
Курс	**3**	семестр	**5**
Трудоемкость в кредитах (зачетных единицах)	**3**		
Виды учебной деятельности	Временной ресурс		
Контактная (аудиторная) работа, ч	Лекции		**16**
	Практические занятия		**-**
	Лабораторные занятия		**32**
	ВСЕГО		**48**
Самостоятельная работа, ч			**60**
ИТОГО, ч			**108**

Вид промежуточной аттестации	**Зачет**	Обеспечивающее подразделение	**ОЭЭ**

И.о. заведующего кафедрой - руководителя ОЭЭ на правах кафедры		Ивашутенко А.С.
Руководитель ООП		Прохоров А.В.
Преподаватель		Хабибулина Н.Ю.

2020 г.

1. Цели освоения дисциплины

Целями освоения дисциплины является формирование у обучающихся определенного ООП (п. 5.4 Общей характеристики ООП) состава компетенций для подготовки к профессиональной деятельности.

Код компетенции	Наименование компетенции	Индикаторы достижения компетенций		Составляющие результатов освоения (дескрипторы компетенции)	
		Код индикатора	Наименование индикатора достижения	Код	Наименование
ОПК(У)-6	Способен исследовать современные проблемы и методы прикладной информатики и развития информационного общества	И.ОПК(У)-6.1	Совершенствует свое представление о современных проблемах прикладной информатики и развития информационного общества	ОПК(У)-6.131	Знает: содержание, объекты и субъекты информационного общества критерии эффективности его функционирования
				ОПК(У)-6.1У1	Умеет: определять актуальные тенденции и проблемы прикладной информатики и развития информационного общества
		И.ОПК(У)-6.2	Осуществляет поиск и анализ применимости методов и средств прикладной информатики для решения прикладных задач различных классов	ОПК(У)-6.231	Знает: современные методы, средства, стандарты информатики для решения прикладных задач различных классов
				ОПК(У)-6.232	Знает: правовые, экономические, социальные и психологические аспекты информатизации деятельности организационно-экономических систем
				ОПК(У)-6.2У1	Умеет: проводить анализ применимости методов и средств прикладной информатики для решения прикладных задач различных классов
ПК(У)-3	Способен выявлять ошибки и неисправности в работе информационных систем, предлагать решения по их устранению, реализовывать технические мероприятия по обеспечению требований к надежности и информационной безопасности	И.ПК(У)-3.2	Реализует технические мероприятия по обеспечению требований к надежности и безопасности информационных систем	ПК(У)-3.2В1	Владеет: методами защиты информации
				ПК(У)-3.2У1	Умеет: выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в информационных системах
				ПК(У)-3.231	Знает: виды угроз и методы обеспечения информационной безопасности корпоративных информационных систем
				ПК(У)-3.232	Знает: программные и аппаратные средства обеспечения информационной безопасности
				ПК(У)-3.2У2	Умеет: применять алгоритмы симметричного и ассиметричного шифрования данных
				ПК(У)-3.233	Знает: алгоритмы защиты данных

2. Место дисциплины (модуля) в структуре ООП

Дисциплина относится к вариативной части Блока 1 учебного плана образовательной программы.

3. Планируемые результаты обучения по дисциплине

После успешного освоения дисциплины будут сформированы результаты обучения:

Планируемые результаты обучения по дисциплине		Индикатор достижения компетенции
Код	**Наименование**	
РД1	Выявлять актуальные тенденции и проблемы информационной безопасности в развитии информационного общества	И.ОПК(У)-6.1
РД2	Выполнять анализ угроз информационной безопасности, их последствий и обосновывать организационно-технические мероприятия по защите информации в информационных системах	И.ПК(У)-3.2
РД3	Обосновывать выбор методов защиты информации и применять их при разработке и использовании информационных систем	И.ОПК(У)-6.2
РД4	Применять программные и аппаратные средства обеспечения информационной безопасности	И.ПК(У)-3.2
РД5	Применять алгоритмы симметричного и ассиметричного шифрования данных	И.ПК(У)-3.2

Оценочные мероприятия текущего контроля и промежуточной аттестации представлены в календарном рейтинг-плане дисциплины.

4. Структура и содержание дисциплины
Основные виды учебной деятельности

Разделы дисциплины	Формируемый результат обучения по дисциплине	Виды учебной деятельности	Объем времени, ч.
Раздел (модуль) 1. Общие вопросы информационной безопасности	РД1 РД2	Лекции	2
		Практические занятия	–
		Лабораторные занятия	4
		Самостоятельная работа	8
Раздел (модуль) 2. Угрозы безопасности	РД1 РД2	Лекции	2
		Практические занятия	–
		Лабораторные занятия	4
		Самостоятельная работа	8
Раздел (модуль) 3. Теоретические основы методов защиты информационных систем	РД3	Лекции	2
		Практические занятия	–
		Лабораторные занятия	4
		Самостоятельная работа	8
Раздел (модуль) 4. Основы криптографии	РД3 РД5	Лекции	2
		Практические занятия	–
		Лабораторные занятия	4
		Самостоятельная работа	8
Раздел (модуль) 5. Методы защиты средств вычислительной техники	РД1 РД3 РД4	Лекции	4
		Практические занятия	–
		Лабораторные занятия	8
		Самостоятельная работа	10
Раздел (модуль) 6. Алгоритмы безопасности в компьютерных сетях	РД4	Лекции	4
		Практические занятия	–
		Лабораторные занятия	8
		Самостоятельная работа	18

Содержание разделов дисциплины:

Раздел 1. ***Общие вопросы информационной безопасности***

Тема лекций:

Основные понятия и определения. Международные стандарты информационного обмена. Требования к защите информации. Комплексность системы защиты информации: инструментальная, структурная, функциональная, временная. Государственная система информационной безопасности. Доктрина информационной безопасности Российской Федерации. Регулирование ИБ АСУ ТП

Названия лабораторных работ:

1. Парольная защита

Раздел 2. ***Угрозы безопасности***

Тема лекций:

Понятие угрозы. Виды противников или «нарушителей». Классификация угроз информационной безопасности. Характер происхождения угроз (умышленные и естественные факторы). Источники угроз. Предпосылки появления угроз. Классы каналов несанкционированного получения информации

Названия лабораторных работ:

1. Архивирование с паролем

Раздел 3. ***Теоретические основы методов защиты информационных систем***

Тема лекций:

Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Формальные модели безопасности. Дискреционная модель. Типизированная матрица доступа. Модель распространения прав доступа Take-Grant. Мандатная модель. Ролевая политика безопасности. Ограничения на области применения формальных моделей

Названия лабораторных работ:

1. Шифр простой замены, таблица Вижинера

Раздел 4. ***Основы криптографии***

Тема лекций:

Методы криптографии. Симметричное и асимметричное шифрование. Алгоритмы шифрования. Электронно-цифровая подпись. Хеширование. Криптографические генераторы случайных чисел. Способы распространения ключей. Обеспечиваемая шифром степень защиты. Криптоанализ и атаки на криптосистемы

Названия лабораторных работ:

1. Обмен ключами по Диффи-Хелману

Раздел 5. ***Методы защиты средств вычислительной техники***

Тема лекций:

Использование защищенных компьютерных систем. Аппаратные и программные средства для защиты компьютерных систем от НСД. Средства операционной системы. Средства резервирования данных. Проверка целостности.

Названия лабораторных работ:

1. Шифр RSA

Раздел 6. ***Алгоритмы безопасности в компьютерных сетях***

Тема лекций:

Межсетевые экраны. Проектирование МЭ. Атаки на сервера. Атаки на рабочие станции. Атака типа «отказ в обслуживании». Протоколирование. Сетевые защищенные протоколы.

Названия лабораторных работ:

1. Проектирование комплексной системы защиты информации объекта энергосистемы.

5. Организация самостоятельной работы студентов

Самостоятельная работа студентов при изучении дисциплины (модуля) предусмотрена в следующих видах и формах:

Основные виды и формы самостоятельной работы

Виды самостоятельной работы	Объем времени, ч
Работа в электронном курсе (изучение теоретического материала, выполнение индивидуальных заданий и контролирующих мероприятий и др.), подготовка к оценивающим мероприятиям (тестам)	12
Изучение тем, вынесенных на самостоятельную проработку. Поиск и обзор литературы и электронных источников информации по индивидуально заданной проблеме курса. Поиск (в том числе перевод текстов с иностранных языков), анализ научных публикаций, структурирование и презентация информации. Примерные темы аналитических обзоров: 1. Современные аппаратно-программные комплексы ЗИ 2. Теоретические основы методов защиты информационных систем 3. Биометрические системы защиты информации 4. Методы стеганографии 5. Исследование принципов работы клавиатурных шпионов и методов борьбы с ними 6. Атаки типа «SQL-инъекция» и методы борьбы с ними. 7. Электронные ключи, электронные замки. 8. Обеспечение информационной безопасности для систем связи и управления в электроэнергетике 9. Модели угроз согласно нормативным документам ФСТЭК России. 10. Обеспечение информационной безопасности для систем связи и управления в электроэнергетике	24
Подготовка к лабораторным работам	16
Подготовка к зачету	8

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Учебно-методическое обеспечение

Основная литература:

1. Мещеряков, Р. В. Безопасность информационных систем : учебное пособие / Р. В. Мещеряков, Е. Е. Мокина; Национальный исследовательский Томский политехнический университет (ТПУ), Институт кибернетики (ИК), Кафедра оптимизации систем управления (ОСУ). —Томск: Изд-во ТПУ, 2013. — URL: http://www.lib.tpu.ru/fulltext2/m/2013/m382.pdf (дата обращения: 22.05.2020) Режим доступа: из корпоративной сети ТПУ. — Текст: электронный.
2. Платонов, Владимир Владимирович. Программно-аппаратные средства защиты информации : учебник в электронном формате / В. В. Платонов. — 2-е изд., стер. — Москва: Академия, 2014. — Высшее образование. —Информационная безопасность. — URL: http://www.lib.tpu.ru/fulltext2/m/2014/FN/fn-99.pdf (дата обращения: 22.05.2020) Режим доступа: из корпоративной сети ТПУ. — Текст: электронный.
3. Бирюков, А. А. Информационная безопасность: защита и нападение : учебник / А. А. Бирюков. — Москва : ДМК Пресс, 2012. — 474 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/39990 (дата обращения: 22.05.2020). — Режим доступа: для авториз. пользователей.

4. Белоус, А. И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения / А. И. Белоус. — Вологда : Инфра-Инженерия, 2020. — 644 с. — ISBN 978-5-9729-0512-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/148386 (дата обращения: 22.05.2020). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

1. Бабаш, А. В. Информационная безопасность : лабораторный практикум : учебное пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. — Москва: КноРус, 2012. — 136 с.: ил. + CD-ROM. — Текст : непосредственный 6 экз.
2. Бузов, Г. А. Защита информации ограниченного доступа от утечки по техническим каналам: Справочное пособие / Бузов Г.А. - Москва :Гор. линия-Телеком, 2015. - 586 с. Текст : электронный. - URL: https://new.znanium.com/catalog/product/895240 (дата обращения: 22.05.2020)
3. Зайцев, А. П. Технические средства и методы защиты информации: Учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В.Мещеряков; Под ред. А.П.Зайцева - 7 изд., исправ. - Москва : Гор. линия-Телеком, 2012. - 442с.; - (Уч. для вузов). - Текст : электронный. - URL: https://new.znanium.com/catalog/product/390284 (дата обращения: 22.05.2020)
4. Защита информации. Inside : информационно-методический журнал / ООО "Издательский Дом "Афина". — Санкт-Петербург: Афина, 2005-2017. - Режим доступа: http://elibrary.ru/title about.asp?id=25917 ; Режим доступа: http://www.inside-zi.ru/ (контент), (дата обращения: 22.05.2020)
5. Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2020. — 184 с. — ISBN 978-5-8114-4291-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://ezproxy.ha.tpu.ru:2225/book/130184 (дата обращения: 22.05.2020). — Режим доступа: для авториз. пользователей.

6.2. Информационное и программное обеспечение

Internet-ресурсы (в т.ч. в среде LMS MOODLE и др. образовательные и библиотечные ресурсы):

1. Каталог по безопасности www.sec.ru.
2. Компьютерная безопасность www.bugtraq.ru
3. «Кибербезопасность – актуальность для современных специалистов энергетиков». - URL:http://cigre.ru/upload/files/news/Презентация_Карантаев_Открытая_лекция_ИБ_в_Электроэнергетике_v1_МЭИ_01.0....pdf
4. Профессиональные базы данных и информационно-справочные системы доступны по ссылке: https://www.lib.tpu.ru/html/irs-and-pdb
5. Полнотекстовые и реферативные базы данных для студентов и сотрудников ТПУ: https://www.lib.tpu.ru/html/full-text-db

Лицензионное программное обеспечение (в соответствии с **Перечнем лицензионного программного обеспечения ТПУ)**:

1. Microsoft Office 2007 Standard Russian Academic
2. Document Foundation Libre Office
3. Microsoft Visual Studio 2019 Community

7. Особые требования к материально-техническому обеспечению дисциплины

В учебном процессе используется следующее лабораторное оборудование для практических и лабораторных занятий:

№	Наименование специальных помещений	Наименование оборудования
1.	Аудитория для проведения учебных занятий всех типов, курсового проектирования, консультаций, текущего контроля и промежуточной аттестации (компьютерный класс) 634034, Томская область, г. Томск, Усова улица, 7 249	Компьютер - 19 шт., Экран Limien Master Control «LMC-100114» - 1 шт., Видеостена - 1шт., проектор – 1 шт. Доска аудиторная настенная - 1 шт., шкаф для документов - 1 шт., полка - 2 шт., комплект учебной мебели на 15 посадочных мест.
2.	Аудитория для проведения учебных занятий всех типов, курсового проектирования, консультаций, текущего контроля и промежуточной аттестации (компьютерный класс) 634034, Томская область, г. Томск, Усова улица, 7 221	Компьютер – 20 шт., видеопроектор - 1 шт., звуковая система - 1 шт. Доска аудиторная настенная - 1 шт., тумба подкатная - 3 шт., комплект учебной мебели на 15 посадочных мест.

Рабочая программа составлена на основе Общей характеристики основной образовательной программы по направлению 09.04.03 Прикладная информатика, специализация «Информационные технологии в электроэнергетике» (приема 2019 г., очно-заочная форма обучения).

Разработчик(и):

Должность	Подпись	ФИО
Соответствует должности - доцент		Хабибулина Н.Ю.

Программа одобрена на заседании Отделения электроэнергетики и электротехники Инженерной школы энергетики (протокол от «27» июня 2019 г. № 6).

И.о. заведующего кафедрой -
руководителя ОЭЭ на правах кафедры
к. т. н, доцент А.С. Ивашутенко

Лист изменений рабочей программы дисциплины:

Учебный год	Содержание /изменение	Обсуждено на заседании Отделения электроэнергетики и электротехники (протокол)
2020/2021	1. Обновлено программное обеспечение 2. Обновлен состав профессиональных баз данных и информационно-справочных систем 3. Обновлено содержание разделов дисциплины 4. Обновлен список литературы, в том числе ссылок ЭБС	протокол от «25» июня 2020 г. № 6