Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сибирский государственный индустриальный университет»

Кафедра прикладных информационных технологий и программирования

УТВЕРЖДАЮ
Проректор по учебной и
воспитательной работе
_____ М.В. Темлянцев
подпись
«____» _____ 20___ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Комплексное обеспечение информационной безопасности

09.04.01 «Информатика и вычислительная техника»
(направленность (профиль): «Информатика и вычислительная техника»)

Квалификация выпускника
Магистр

Форма обучения
Очно-заочная форма

Срок обучения: 2 года 3 месяца

Год начала подготовки 2022

Новокузнецк
2022

1 Цели и задачи освоения учебной дисциплины

Целями учебной дисциплины являются:

– формирование у обучающихся знаний в области теоретических основ информационной безопасности и навыков практического обеспечения защиты информации в организации.

Задачами учебной дисциплины являются:

– изучить основные задачи в рамках общей проблемы обеспечения информационной безопасности в организации, решаемых организационно-правовыми, техническими и программно-аппаратными средствами защиты информации;
– изучить нормативные и методические материалы по методам, способам и средствам обеспечения информационной безопасности телекоммуникационных систем;
– изучить возможности современных технических и программно-аппаратных средств защиты информации;
– обеспечить знание обучающимися принципов и методов применения технических и программно-аппаратных средств защиты информации в информационно-телекоммуникационных системах;
– научиться использовать современные пакеты прикладных программ для решения типовых задач, связанных с анализом и синтезом элементов защищенных телекоммуникационных систем;
– научиться практически решать задачи защиты данных;
– выработать навыки работы с современными техническими и программно-аппаратными средствами защиты информации;
– научиться применять системный подход к обеспечению информационной безопасности телекоммуникационных систем.

2 Место учебной дисциплины в структуре ООП по направлению подготовки (специальности)

Учебная дисциплина относится к учебным дисциплинам части, формируемой участниками образовательных отношений **Блока 1 «Дисциплины (модули)»** ООП по направлению подготовки (специальности) 09.04.01 «Информатика и вычислительная техника».

Учебная дисциплина базируется на предварительном усвоении обучающимися учебных дисциплин:

– Математические и инструментальные методы анализа данных;
– Методология и технология проектирования информационных систем;
– Технология разработки программного обеспечения.

Учебная дисциплина дополняет знания, умения и навыки, получаемые по одновременно изучаемым и последующим дисциплинам:

– Управление разработкой программного обеспечения;

– Управление требованиями к программному обеспечению;
– Проектно-технологическая практика;
– Преддипломная практика;
– Выполнение и защита выпускной квалификационной работы.

3 Планируемые результаты обучения по учебной дисциплине

Процесс изучения учебной дисциплины направлен на формирование следующих компетенций:

– Профессиональные компетенции

Наименование категории (группы) ПК	Код и наименование ПК	Код и наименование индикатора достижения ПК	Планируемые результаты обучения
	ПК-1: Способен участвовать в руководстве программно-техническими ресурсами	ПК-1.1 Принимает участие в выборе инструментальных средств разработки программного обеспечения	– знать: методы и приема сбора требований пользователей. – уметь: анализировать требования к программному обеспечению, оценивать стойкость различных паролей и методов шифрования. – владеть: навыками оценки сроков и трудоемкости реализации требований к программному обеспечению.
		ПК-1.2 Принимает участие в руководстве разработкой программного обеспечения и использования инфраструктуры	– знать: методологию, этапы, принципы разработки программного обеспечения, принципы и методы синхронизации программы информационной безопасности с жизненным циклом ПО. – уметь: выбирать

			модель жизненного цикла ПО, определять потенциальные угрозы информационной безопасности для разрабатываемого ПО, определять необходимые методы, средства и инструменты информационной защиты. – владеть: навыками планирования, организации и управления разработкой ПО, составления программной документации.
	ПК-2: Способен разрабатывать и применять алгоритмы интеллектуального анализа больших объемов данных для управления технологическими системами	ПК-2.2 Собирает данные из различных источников и осуществляет их подготовку для анализа	– знать: стандарты в области защиты информации; возможности методов и средств криптографического преобразования и электронной цифровой подписи данных; основные концепциях и модели компьютерной безопасности; технологии построения защищенных систем. – уметь: различать объекты, субъекты, модули и процессы компьютерной системы; использовать дискреционный и мандатный методы контроля доступа к информации. – владеть:

			навыками постановки целей разграничения доступа пользователей к информации, управления их полномочиями и использования парольной защиты; настройки службы обеспечения сетевой безопасности.

4 Объем и содержание учебной дисциплины

Учебные занятия по учебной дисциплине проводятся в форме контактной работы и в форме самостоятельной работы обучающихся.

Контактная работа обучающихся с педагогическим работником включает в себя занятия лекционного типа (лекции), занятия семинарского типа (семинары, практические занятия, практикумы), промежуточную аттестацию обучающихся и иную контактную работу, предусматривающую групповую или индивидуальную работу обучающихся с педагогическим работником. Контактная работа обучающихся с педагогическим работником может быть аудиторной, внеаудиторной, а также проводиться в электронной информационно-образовательной среде.

Объем учебной дисциплины

Семестр / курс		***ИТОГО***	***2 семестр***
Форма промежуточной аттестации			*экзамен*
Трудоёмкость	*академ. час.*	***180***	*180*
	зачетных единиц	***5***	*5*
Лекции, *академ. час.*		***6***	*6*
в форме практической подготовки		***0***	*0*
Лабораторные работы, *академ. час.*		***0***	*0*
в форме практической подготовки		***0***	*0*
Практические занятия, *академ. час.*		***8***	*8*
в форме практической подготовки		***0***	*0*
Курсовая работа / проект, *академ. час.*		***0***	*0*
в форме практической подготовки		***0***	*0*
Консультации, *академ. час.*		***0***	*0*
в форме практической подготовки		***0***	*0*
Самостоятельная работа, *академ. час.*		***130***	*130*
в форме практической подготовки		***0***	*0*
Контроль, *академ. час.*		***36***	*36*
в форме практической подготовки		***0***	*0*

Содержание учебной дисциплины

Раздел 1 Методологические основы обеспечения информационной безопасности;

Тема 1.1 Проблемы обеспечения информационной безопасности и пути их решения (Особенности обеспечения информационной безопасности в различных сферах жизнедеятельности общества и государства. Основные направления обеспечения информационной безопасности);

Тема 1.2 Угрозы информационной безопасности и оценка вероятности их реализации (Объекты, угрозы и источники угроз информационной безопасности. Возможные последствия угроз информационной безопасности. Методы и средства предотвращения и нейтрализации угроз информационной безопасности);

Тема 1.3 Основные свойства и показатели эффективности системы защиты информации (Обеспечение защиты информации на практике. Факторы, влияющие на уровень защиты информации);

Раздел 2 Комплексный подход к обеспечению информационной безопасности объекта;

Тема 2.1 Анализ способов нарушений информационной безопасности (Классификация угроз. Степени и проявления ущерба. Защита информации в локальных и глобальных компьютерных сетях. Электронная подпись);

Тема 2.2 Управление информационной безопасностью (Система управления информационной безопасностью. Криптографические и статистические методы защиты. Типовые подсистемы и решения обеспечения информационной безопасности).

5 Перечень тем лекций

№ раздела / темы дисциплины	Темы лекций	Трудоемкость, *академ.час*	
		всего	**в форме практической подготовки**
Раздел 1.	Методологические основы обеспечения информационной безопасности	2	
Раздел 2.	Комплексный подход к обеспечению информационной безопасности объекта	4	
Итого:		**6**	**0**

6 Перечень тем практических занятий (семинаров)

№ раздела / темы дисциплины	Темы практических занятий (семинаров)	Трудоемкость, *академ.час*	
		всего	**в форме**

			практической подготовки
Раздел 1.	Определение способов защиты информации: составление списка возможных атак и стратегий осуществления этих атак	2	
Раздел 2.	Анализ таксономии причин нарушений безопасности. Использование методов разработки защищенных компьютерных систем	6	
Итого:		**8**	**0**

7 Перечень тем лабораторных работ

№ раздела / темы дисциплины	**Темы лабораторных работ**	**Трудоемкость, *академ.час***	
		всего	**в форме практической подготовки**
	Отсутствуют		
Итого:		**0**	**0**

8 Перечень тем курсовых работ (проектов)

№ раздела / темы дисциплины	**Темы курсовых работ (проектов)**	**Трудоемкость, *академ.час***	
		всего	**в форме практической подготовки**
	Отсутствуют		
Итого:		**0**	**0**

9 Виды самостоятельной работы

№ раздела / темы дисциплины	**Виды самостоятельной работы**	**Трудоемкость, *академ.час***	
		всего	**в форме практической подготовки**
Раздел 1.	1. Изучение лекционного материала; 2. Подготовка к практическому занятию; 3. Прохождение тестирования.	58	
Раздел 2.	1. Изучение лекционного материала; 2. Подготовка к практическому занятию; 3. Прохождение	72	

	тестирования.		
Контроль	*Подготовка к экзамену*	36	
Итого:		**166**	**0**

10 Учебно-методическое и информационное обеспечение учебной дисциплины

а) литература:

1 Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. – 2-е изд. – Москва : Издательство Юрайт, 2020. – 473 с. – ISBN 978-5-534-12474-3. – URL: https://urait.ru/bcode/450277 (дата обращения: 19.03.2022);

2 Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. – Москва : Издательство Юрайт, 2020. – 349 с. – URL: https://urait.ru/bcode/450998 (дата обращения: 19.03.2022);

3 Информационное право. Практикум : учебное пособие для вузов / Н. Н. Ковалева, Н. А. Жирнова, Ю. М. Тугушева, Е. В. Холодная ; под редакцией Н. Н. Ковалевой. – Москва : Издательство Юрайт, 2020. – 159 с. – ISBN 978-5-534-12442-2. – URL: https://urait.ru/bcode/449378 (дата обращения: 19.03.2022);

4 Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. – Москва : Издательство Юрайт, 2020. – 325 с. – ISBN 978-5-534-03600-8. – URL: https://urait.ru/bcode/450371 (дата обращения: 19.03.2022);

5 Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование : учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. – Москва : Издательство Юрайт, 2020. – 220 с. – ISBN 978-5-9916-9244-1. – URL: https://urait.ru/bcode/452871 (дата обращения: 19.03.2022);

6 Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. – Москва : Издательство Юрайт, 2020. – 342 с. – ISBN 978-5-534-05142-1. – URL: https://urait.ru/bcode/454453 (дата обращения: 19.03.2022);

7 Шилов, А. К. Управление информационной безопасностью : учебное пособие / А. К. Шилов ; Южный федеральный университет. – Москва : ЮФУ, 2018. – 120 с. – ISBN 978-5-9275-2742-7. – URL: https://www.studentlibrary.ru/book/ISBN9785927527427.html (дата обращения: 19.03.2022);

8 Ярочкин, В.И. Информационная безопасность : учебник для вузов / Ярочкин В. И. – Москва : Академический Проект, 2020. – 544 с. – ISBN 978-5-8291-3031-2. – URL:

https://www.studentlibrary.ru/book/ISBN9785829130312.html (дата обращения: 19.03.2022);

9 Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика : учебное пособие / В.Я. Ищейнов. – Москва : Берлин : Директ-Медиа, 2020. – 271 с. – ISBN 978-5-4499-0496-6. – URL: https://biblioclub.ru/index.php?page=book&id=571485 (дата обращения: 19.03.2022).

б) ресурсы информационно-телекоммуникационной сети «Интернет»:

1 Консультант студента. Электронная библиотека технического ВУЗа : электронно-библиотечная система / ООО «Политехресурс». – Москва, [200 –]. – URL: http://www.studentlibrary.ru. – Режим доступа: для авторизир. пользователей;

2 ЛАНЬ : электронно-библиотечная система : [коллекция «Инженерно-технические науки»] / ООО «Издательство Лань». – Санкт-Петербург, [200 –]. – URL: http://e.lanbook.com. – Режим доступа: для авторизир. пользователей;

3 НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА eLIBRARY.RU : база данных / ООО «НЭБ». – Москва, [200 –]. – URL: http://elibrary.ru. – Режим доступа: по подписке;

4 Образовательная платформа ЮРАЙТ / ООО «Электронное издательство Юрайт». – Москва, [200 –]. – URL: https://urait.ru. – Режим доступа: для авторизир. пользователей;

5 Университетская библиотека онлайн : электронно-библиотечная система / ООО «Директ-Медиа». – Москва, [200 –]. – URL: http://www.biblioclub.ru. – Режим доступа: для авторизир. пользователей;

6 Электронная библиотека // Научно-техническая библиотека СибГИУ : сайт. – Новокузнецк, [200 –]. – URL: http://library.sibsiu.ru/LibrELibraryFullText.asp. – Режим доступа: для авторизир. пользователей;

7 Электронный каталог : сайт / Научно-техническая библиотека СибГИУ. – Новокузнецк, [199 –]. – URL: http://libr.sibsiu.ru.

в) лицензионное и свободно распространяемое программное обеспечение:

– Adobe Acrobat Reader;
– Kaspersky Endpoint Security;
– Microsoft Office 2010;
– Microsoft Visual Studio Community;
– Microsoft Windows 7.

г) базы данных и информационно-справочные системы:

1 КонсультантПлюс : справочно-правовая система / ООО «Информационный центр АНВИК». – Новокузнецк, [199 –]. – Режим доступа: компьютерная сеть библиотеки Сиб. гос. индустр. ун-та.;

2 Система ГАРАНТ : электронный периодический справочник / ООО «Правовой центр «Гарант». – Кемерово, [200 –]. – Режим доступа: компьютерная сеть Сиб. гос. индустр. ун-та.;

3 Техэксперт : информационно-справочная система / ООО «Группа компаний «Кодекс». – Кемерово, [200 –]. – Режим доступа: компьютерная сеть Сиб. гос. индустр. ун-та.;

4 Электронный реферативный журнал (ЭлРЖ) : база данных / ВИНИТИ РАН. – Москва, [200 –]. – Режим доступа: компьютерная сеть библиотеки Сиб. гос. индустр. ун-та.

11 Материально-техническое обеспечение учебной дисциплины

Материально-техническое обеспечение учебной дисциплины включает учебные аудитории, оснащенные оборудованием, компьютерной техникой, и техническими средствами обучения, в том числе:

- учебную аудиторию для проведения занятий лекционного типа, оборудованную учебной доской, экраном и мультимедийным проектором;
- учебную аудиторию для проведения занятий семинарского типа (практических занятий);
- учебную аудиторию (помещения) для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду, научно-техническую библиотеку СибГИУ.
- учебную аудиторию (помещения) для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации;

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению подготовки (специальности) 09.04.01 «Информатика и вычислительная техника».

Составитель(и):

доцент Пермякова Елена Павловна (кафедра прикладных информационных технологий и программирования).

Рабочая программа дисциплины рассмотрена и утверждена на заседании кафедры.

Приложение А

Аннотация
рабочей программы дисциплины «Комплексное обеспечение информационной безопасности»

по направлению подготовки (специальности)
09.04.01 «Информатика и вычислительная техника»
(направленность (профиль): «Информатика и вычислительная техника»)
форма обучения – Очно-заочная форма

1 Цели и задачи освоения учебной дисциплины

Целями учебной дисциплины являются:

– формирование у обучающихся знаний в области теоретических основ информационной безопасности и навыков практического обеспечения защиты информации в организации.

Задачами учебной дисциплины являются:

– изучить основные задачи в рамках общей проблемы обеспечения информационной безопасности в организации, решаемых организационно-правовыми, техническими и программно-аппаратными средствами защиты информации;
– изучить нормативные и методические материалы по методам, способам и средствам обеспечения информационной безопасности телекоммуникационных систем;
– изучить возможности современных технических и программно-аппаратных средств защиты информации;
– обеспечить знание обучающимися принципов и методов применения технических и программно-аппаратных средств защиты информации в информационно-телекоммуникационных системах;
– научиться использовать современные пакеты прикладных программ для решения типовых задач, связанных с анализом и синтезом элементов защищенных телекоммуникационных систем;
– научиться практически решать задачи защиты данных;
– выработать навыки работы с современными техническими и программно-аппаратными средствами защиты информации;
– научиться применять системный подход к обеспечению информационной безопасности телекоммуникационных систем.

2 Место учебной дисциплины в структуре ООП по направлению подготовки (специальности)

Учебная дисциплина относится к учебным дисциплинам части, формируемой участниками образовательных отношений **Блока 1**

«Дисциплины (модули)» ООП по направлению подготовки (специальности) 09.04.01 «Информатика и вычислительная техника».

Учебная дисциплина базируется на предварительном усвоении обучающимися учебных дисциплин:

– Математические и инструментальные методы анализа данных;
– Методология и технология проектирования информационных систем;
– Технология разработки программного обеспечения.

Учебная дисциплина дополняет знания, умения и навыки, получаемые по одновременно изучаемым и последующим дисциплинам:

– Управление разработкой программного обеспечения;
– Управление требованиями к программному обеспечению;
– Проектно-технологическая практика;
– Преддипломная практика;
– Выполнение и защита выпускной квалификационной работы.

3 Планируемые результаты обучения по учебной дисциплине

Процесс изучения учебной дисциплины направлен на формирование следующих компетенций:

– Профессиональные компетенции

Наименование категории (группы) ПК	Код и наименование ПК	Код и наименование индикатора достижения ПК	Планируемые результаты обучения
	ПК-1: Способен участвовать в руководстве программно-техническими ресурсами	ПК-1.1 Принимает участие в выборе инструментальных средств разработки программного обеспечения	– знать: методы и приема сбора требований пользователей. – уметь: анализировать требования к программному обеспечению, оценивать стойкость различных паролей и методов шифрования. – владеть: навыками оценки сроков и трудоемкости реализации требований к программному обеспечению.
		ПК-1.2 Принимает участие в руководстве	– знать: методологию, этапы, принципы

		разработкой программного обеспечения и использования инфраструктуры	разработки программного обеспечения, принципы и методы синхронизации программы информационной безопасности с жизненным циклом ПО. – уметь: выбирать модель жизненного цикла ПО, определять потенциальные угрозы информационной безопасности для разрабатываемого ПО, определять необходимые методы, средства и инструменты информационной защиты. – владеть: навыками планирования, организации и управления разработкой ПО, составления программной документации.
	ПК-2: Способен разрабатывать и применять алгоритмы интеллектуального анализа больших объемов данных для управления технологическими системами	ПК-2.2 Собирает данные из различных источников и осуществляет их подготовку для анализа	– знать: стандарты в области защиты информации; возможности методов и средств криптографического преобразования и электронной цифровой подписи данных; основные концепциях и модели компьютерной безопасности; технологии построения защищенных

			систем. – уметь: различать объекты, субъекты, модули и процессы компьютерной системы; использовать дискреционный и мандатный методы контроля доступа к информации. – владеть: навыками постановки целей разграничения доступа пользователей к информации, управления их полномочиями и использования парольной защиты; настройки службы обеспечения сетевой безопасности.

4 Объем учебной дисциплины

Семестр / курс		***ИТОГО***	***2 семестр***
Форма промежуточной аттестации			*экзамен*
Трудоёмкость	*академ. час.*	***180***	*180*
	зачетных единиц	***5***	*5*
Лекции, *академ. час.*		***6***	*6*
в форме практической подготовки		***0***	*0*
Лабораторные работы, *академ. час.*		***0***	*0*
в форме практической подготовки		***0***	*0*
Практические занятия, *академ. час.*		***8***	*8*
в форме практической подготовки		***0***	*0*
Курсовая работа / проект, *академ. час.*		***0***	*0*
в форме практической подготовки		***0***	*0*
Консультации, *академ. час.*		***0***	*0*
в форме практической подготовки		***0***	*0*
Самостоятельная работа, *академ. час.*		***130***	*130*
в форме практической подготовки		***0***	*0*
Контроль, *академ. час.*		***36***	*36*
в форме практической подготовки		***0***	*0*

5 Краткое содержание учебной дисциплины

В структуре учебной дисциплины выделяются следующие основные разделы (темы):

Раздел 1 Методологические основы обеспечения информационной безопасности;

Тема 1.1 Проблемы обеспечения информационной безопасности и пути их решения (Особенности обеспечения информационной безопасности в различных сферах жизнедеятельности общества и государства. Основные направления обеспечения информационной безопасности);

Тема 1.2 Угрозы информационной безопасности и оценка вероятности их реализации (Объекты, угрозы и источники угроз информационной безопасности. Возможные последствия угроз информационной безопасности. Методы и средства предотвращения и нейтрализации угроз информационной безопасности);

Тема 1.3 Основные свойства и показатели эффективности системы защиты информации (Обеспечение защиты информации на практике. Факторы, влияющие на уровень защиты информации);

Раздел 2 Комплексный подход к обеспечению информационной безопасности объекта;

Тема 2.1 Анализ способов нарушений информационной безопасности (Классификация угроз. Степени и проявления ущерба. Защита информации в локальных и глобальных компьютерных сетях. Электронная подпись);

Тема 2.2 Управление информационной безопасностью (Система управления информационной безопасностью. Криптографические и статистические методы защиты. Типовые подсистемы и решения обеспечения информационной безопасности).

6 Составитель(и):

доцент Пермякова Елена Павловна (кафедра прикладных информационных технологий и программирования).