

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
Директор института
информационных технологий и
автоматизированных систем
_____ Л.Д. Павлова
подпись
« ____ » _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Комплексное обеспечение информационной безопасности

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

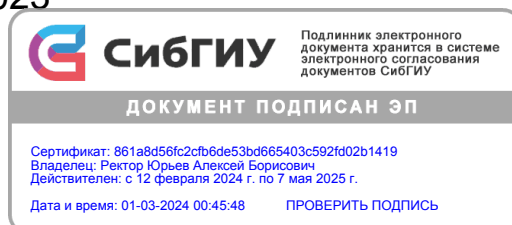
Квалификация выпускника
Магистр

Форма обучения
Очная форма

Срок обучения: 2 года

Год начала подготовки 2023

Новокузнецк
2023



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;
- 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:

- Технологии разработки программного обеспечения;
- Дисциплина не подразумевает проведение входного контроля и рассчитана на обучающегося 1 курса, поступившего в университет в соответствии с Правилами приема в СибГИУ.

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

- Управление разработкой программного обеспечения;
- Методы и инструменты цифровой трансформации;
- Стандартизация и сертификация программных продуктов;
- 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 управлении проектированием компьютерного программного обеспечения	ПК-1.1 Анализирует архитектуру компьютерного программного обеспечения	– знать: архитектурные принципы разработки программного обеспечения. – уметь: определять объекты защиты данных, анализировать возможности осуществления атак. – владеть: навыками определения однозначного соответствия защищаемых ресурсов и характеристик безопасности.
		ПК-1.2 Проектирует структуры баз данных и оценивает их качество	– знать: методологию, этапы, принципы разработки программного обеспечения и баз данных, принципы и методы синхронизации программы информационной безопасности с жизненным циклом ПО. – уметь: определять потенциальные угрозы информационной безопасности для разрабатываемого ПО и баз данных, определять необходимые методы,

			<p>средства и инструменты информационной защиты.</p> <p>– владеть: навыками планирования, организации и управления разработкой ПО.</p>
	<p>ПК-2: Способен разрабатывать и применять алгоритмы интеллектуального анализа больших объемов данных для управления технологическими системами</p>	<p>ПК-2.2 Собирает данные из различных источников и осуществляет их подготовку для анализа</p>	<p>– знать: принципы и методы информационной безопасности на разных уровнях управления организации.</p> <p>– уметь: анализировать и оценивать угрозы безопасности в организации, строить модель нарушителя, разрабатывать модель угроз информационной безопасности.</p> <p>– владеть: навыками постановки целей разграничения доступа пользователей к информации, управления их полномочиями и использования парольной защиты.</p>

4 Объем и содержание учебной дисциплины

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

Контактная работа включает в себя занятия лекционного типа (лекции), занятия семинарского типа (семинары, практические занятия, практикумы), промежуточную аттестацию обучающихся и иные формы взаимодействия обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации ООП на иных условиях, в том числе при проведении промежуточной аттестации обучающихся. Контактная работа может проводиться с применением электронного обучения, дистанционных образовательных технологий.

Объем учебной дисциплины

Семестр / курс		ИТОГО	2 семестр
Форма промежуточной аттестации			экзамен
Трудоёмкость	<i>академ. час.</i>	144	144
	<i>зачетных единиц</i>	4	4
Лекции, <i>академ. час.</i>		16	16
в форме практической подготовки		0	0
Лабораторные работы, <i>академ. час.</i>		0	0
в форме практической подготовки		0	0
Практические занятия, <i>академ. час.</i>		16	16
в форме практической подготовки		0	0
Курсовая работа / проект, <i>академ. час.</i>		0	0
в форме практической подготовки		0	0
Консультации, <i>академ. час.</i>		0	0
в форме практической подготовки		0	0
Самостоятельная работа, <i>академ. час.</i>		76	76
в форме практической подготовки		0	0
Контроль, <i>академ. час.</i>		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 Основные 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, <i>академ. час</i>	
		всего	в форме практической подготовки
Раздел 1.	Методологические основы обеспечения информационной безопасности	8	
Раздел 2.	Комплексный подход к обеспечению информационной безопасности объекта	8	
Итого:		16	0

6 Перечень тем практических занятий (семинаров)

№ раздела / темы дисциплины	Темы практических занятий (семинаров)	Трудоемкость, <i>академ. час</i>	
		всего	в форме практической подготовки
Раздел 1.	Определение способов защиты информации: составление списка возможных атак и стратегий осуществления этих атак	6	
Раздел 2.	Анализ таксономии причин нарушений безопасности. Использование методов разработки защищенных компьютерных систем	10	
Итого:		16	0

7 Перечень тем лабораторных работ

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

8 Перечень тем курсовых работ (проектов)

№ раздела / темы дисциплины	Темы курсовых работ (проектов)	Трудоемкость, <i>академ. час</i>	
		всего	в форме

			практической подготовки
	<i>Отсутствуют</i>		
Итого:		0	0

9 Виды самостоятельной работы

№ раздела / темы дисциплины	Виды самостоятельной работы	Трудоемкость, <i>академ. час</i>	
		всего	в форме практической подготовки
Раздел 1.	1. Изучение лекционного материала; 2. Подготовка к практическому занятию; 3. Прохождение тестирования.	38	
Раздел 2.	1. Изучение лекционного материала; 2. Подготовка к практическому занятию; 3. Прохождение тестирования.	38	
<i>Контроль</i>	<i>Подготовка к экзамену</i>	36	
Итого:		112	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: 24.04.2023);

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: 24.04.2023);

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: 24.04.2023);

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: 24.04.2023);

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: 24.04.2023);

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: 24.04.2023);

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: 24.04.2023);

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: 24.04.2023);

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: 24.04.2023).

б) ресурсы информационно-телекоммуникационной сети «Интернет»:

1 Консультант студента : электронно-библиотечная система / ООО «КОНСУЛЬТАНТ СТУДЕНТА». – 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 Национальная электронная библиотека (НЭБ) : информационная система / ФГБУ «РГБ». – Москва, [2015 –]. – URL: <http://rusneb.ru>. – Режим доступа: по подписке;

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

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

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

8 Электронные периодические издания ИВИС : универсальная база данных / ООО «ИВИС». – Москва, [200 –]. – URL: <http://eivis.ru>. – Режим доступа: по подписке;

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

в) лицензионное и свободно распространяемое программное обеспечение:

- Astra Linux Special Edition;
- LibreOffice;
- Microsoft Office;
- Microsoft Windows.

г) базы данных и информационно-справочные системы:

1 ГАРАНТ : справочно-правовая система / ООО «Правовой центр «Гарант». – Кемерово, [200 –]. – Режим доступа: компьютерная сеть Сиб. гос. индустр. ун-та.;

2 КонсультантПлюс : справочно-правовая система / ООО «Информационный центр АНВИК». – Новокузнецк, [199 –]. – Режим доступа: компьютерная сеть библиотеки 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.

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

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 – Очная 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;
- 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:

- Технологии разработки программного обеспечения;

- Дисциплина не подразумевает проведение входного контроля и рассчитана на обучающегося 1 курса, поступившего в университет в соответствии с Правилами приема в СибГИУ.

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

- Управление разработкой программного обеспечения;
- Методы и инструменты цифровой трансформации;
- Стандартизация и сертификация программных продуктов;
- 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 управлении проектированием компьютерного программного обеспечения	ПК-1.1 Анализирует архитектуру компьютерного программного обеспечения	<ul style="list-style-type: none"> – знать: архитектурные принципы разработки программного обеспечения. – уметь: определять объекты защиты данных, анализировать возможности осуществления атак. – владеть: навыками определения однозначного соответствия защищаемых ресурсов и характеристик безопасности.
		ПК-1.2 Проектирует структуры баз данных и оценивает их качество	<ul style="list-style-type: none"> – знать: методологию, этапы, принципы разработки программного обеспечения и баз данных, принципы и методы синхронизации программы информационной безопасности с

			<p>жизненным циклом ПО.</p> <p>– уметь: определять потенциальные угрозы информационной безопасности для разрабатываемого ПО и баз данных, определять необходимые методы, средства и инструменты информационной защиты.</p> <p>– владеть: навыками планирования, организации и управления разработкой ПО.</p>
	<p>ПК-2: Способен разрабатывать и применять алгоритмы интеллектуального анализа больших объемов данных для управления технологическими системами</p>	<p>ПК-2.2 Собирает данные из различных источников и осуществляет их подготовку для анализа</p>	<p>– знать: принципы и методы информационной безопасности на разных уровнях управления организации.</p> <p>– уметь: анализировать и оценивать угрозы безопасности в организации, строить модель нарушителя, разрабатывать модель угроз информационной безопасности.</p> <p>– владеть: навыками постановки целей разграничения доступа пользователей к информации, управления их полномочиями и использования парольной защиты.</p>

4 Объем учебной дисциплины

Семестр / курс	ИТОГО	2 семестр
Форма промежуточной аттестации		экзамен

Трудоёмкость	<i>академ. час.</i>	144	144
	<i>зачетных единиц</i>	4	4
Лекции, <i>академ. час.</i>		16	16
в форме практической подготовки		0	0
Лабораторные работы, <i>академ. час.</i>		0	0
в форме практической подготовки		0	0
Практические занятия, <i>академ. час.</i>		16	16
в форме практической подготовки		0	0
Курсовая работа / проект, <i>академ. час.</i>		0	0
в форме практической подготовки		0	0
Консультации, <i>академ. час.</i>		0	0
в форме практической подготовки		0	0
Самостоятельная работа, <i>академ. час.</i>		76	76
в форме практической подготовки		0	0
Контроль, <i>академ. час.</i>		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 Основные 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).