

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сибирский государственный индустриальный университет»

Кафедра автоматизации и информационных систем

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность и защита информации

09.03.02 «Информационные системы и технологии»
(направленность (профиль): «Информационные системы и технологии»)

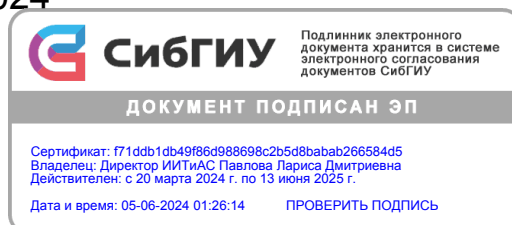
Квалификация выпускника
Бакалавр

Форма обучения
Заочная форма

Срок обучения: 4 года 6 месяцев

Год начала подготовки 2024

Новокузнецк
2024



1 Цели и задачи освоения учебной дисциплины

Целями учебной дисциплины являются:

- изучение теоретических и прикладных аспектов информационной безопасности;
- знакомство с базовыми технологиями защиты информации в информационных системах.

Задачами учебной дисциплины являются:

- изучение типовых механизмов обеспечения безопасности информационных систем;
- получение навыков использования криптографических средств защиты данных в приложениях.

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

Учебная дисциплина относится к учебным дисциплинам обязательной части **Блока 1 «Дисциплины (модули)»** ООП по направлению подготовки (специальности) 09.03.02 «Информационные системы и технологии».

Учебная дисциплина базируется на предварительном усвоении обучающимися учебных дисциплин:

- Математика;
- Информатика;
- Основы программирования;
- Технологии программирования.

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

- Проектирование информационно-управляющих систем;
- Программное обеспечение информационно-управляющих систем.

3 Планируемые результаты обучения по учебной дисциплине

Процесс изучения учебной дисциплины направлен на формирование следующих компетенций:

– Общепрофессиональные компетенции

Наименование категории (группы) ОПК	Код и наименование ОПК	Код и наименование индикатора достижения ОПК	Планируемые результаты обучения
	ОПК-2: Способен понимать принципы работы современных информационных технологий и	ОПК-2.3 Применяет современные информационные технологии и программные средства при	– знать: информационные технологии и программные средства обеспечения

	программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности	решении прикладных задач	информационной безопасности. – уметь: проектировать многоуровневые системы защиты информации.
	ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.2 Понимает и использует принципы защиты информации и обеспечивает информационную безопасность	– знать: методы, подходы и принципы защиты данных в информационных системах. – уметь: проектировать и реализовывать прикладные решения в области защиты данных.

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

Сессия / курс		ИТОГО	2 сессия / 4 курс	3 сессия / 4 курс
Форма промежуточной аттестации				<i>экзамен</i>
Трудоёмкость	<i>академ. час.</i>	144	36	108
	<i>зачетных единиц</i>	4	1	3
Лекции, академ. час.		2	2	0

в форме практической подготовки	0	0	0
Лабораторные работы, <i>академ. час.</i>	0	0	0
в форме практической подготовки	0	0	0
Практические занятия, <i>академ. час.</i>	2	0	2
в форме практической подготовки	0	0	0
Курсовая работа / проект, <i>академ. час.</i>	0	0	0
в форме практической подготовки	0	0	0
Консультации, <i>академ. час.</i>	0	0	0
в форме практической подготовки	0	0	0
Самостоятельная работа, <i>академ. час.</i>	131	34	97
в форме практической подготовки	0	0	0
Контроль, <i>академ. час.</i>	9	0	9
в форме практической подготовки	0	0	0

Содержание учебной дисциплины

Раздел 1 Информационная безопасность;

Тема 1.1 Термины и определения (понятия информационной безопасности, конфиденциальность, целостность, доступность, уязвимость, комплексная защита, риски);

Тема 1.2 Типовые проблемы безопасности (типовые уязвимости информационных систем, phishing - атаки, spoofing атаки, poisoning - атаки, сетевой флуд, arp, ip spoofing (poisoning), отказ в обслуживании);

Тема 1.3 Безопасность программного обеспечения (атаки на программное обеспечение, внедрение внешнего кода, атаки crossscripting и injection (SQL injection), переполнение буфера, атаки переполнения буфера, принципы безопасного программирования);

Раздел 2 Элементы криптографии;

Тема 2.1 Введение в криптографию (история криптографии, логические и криптозащиты (защиты Кирхгофа), перестановочные, подстановочные шифры, примеры логических защит);

Тема 2.2 симметричная криптография (криптозащиты, блочные и поточные схемы шифрования, принципы реализации блочных и поточных защит с закрытым ключом, схема Фейстеля, алгоритмы Triple DES, Rijndael (AES));

Тема 2.3 односторонние хэш функции (задачи хэширования данных, контрольные суммы, односторонние хэш функции, алгоритмы md5, sha1);

Тема 2.4 асимметричная криптография (идея открытого ключа, простые числа и преобразования, алгоритм RSA (Rivest, Shamir, Adelman), протокол Диффи - Хеллмана);

Тема 2.5 электронная цифровая подпись (идея электронной цифровой подписи, цифровые сертификаты, схемы с посредником, алгоритмы RSA, DSA в системах с цифровой подписью);

Тема 2.6 аутентификация и авторизация (системы аутентификации и авторизации, задачи, технологии, реализация подсистем аутентификации и авторизации).

5 Перечень тем лекций

№ раздела / темы дисциплины	Темы лекций	Трудоемкость, <i>академ. час</i>	
		всего	в форме практической подготовки
Раздел 1.	Информационная безопасность		
Тема 1.1.	Термины и определения	2	
Итого:		2	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.	Информационная безопасность		
Тема 1.1.	Использование инструментов анализа и мониторинга сетевого трафика. Cisco packet tracer, wireshark, nmap. Анализ сетевого трафика.	2	
Итого:		2	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. Оформление отчета о практической работе; 3. Подготовка к практическому занятию; 4. Прохождение тестирования.	60	
Раздел 2.	1. Изучение теоретического материала; 2. Контрольная работа; 3. Прохождение тестирования.	71	
<i>Контроль</i>	<i>Подготовка к экзамену</i>	9	
Итого:		140	0

10 Учебно-методическое и информационное обеспечение учебной дисциплины

а) литература:

1 Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. – Москва : Издательство Юрайт, 2023. – 2-е изд., перераб. и доп. – 277 с. – ISBN 978-5-534-16450-3. – URL: <https://urait.ru/bcode/531084> (дата обращения: 03.06.2024);

2 Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. – Москва : Издательство Юрайт, 2023. – 325 с. – ISBN 978-5-534-03600-8. – URL: <https://urait.ru/bcode/511239> (дата обращения: 03.06.2024);

3 Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. – Москва : Издательство Юрайт, 2023. – 342 с. – ISBN 978-5-534-05142-1. – URL: <https://urait.ru/bcode/515435> (дата обращения: 03.06.2024).

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 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: <https://biblioclub.ru>. – Режим доступа: для авторизир. пользователей. – URL: <http://www.biblioclub.ru>;

6 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>;

7 Электронная библиотека УМЦ ЖДТ : [коллекция «Эксплуатация железных дорог»] / ФГБУ ДПО «Учебно-методический центр по образованию на железнодорожном транспорте». – Москва, [2013 –]. – URL: <https://umczdt.ru/books/>. – Режим доступа: для авторизир. пользователей;

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:

- 7-Zip;
- Adobe Acrobat Reader;
- Astra Linux Special Edition;
- Kaspersky Endpoint Security;
- Microsoft Office;
- Microsoft Windows;
- OnlyOffice;
- Р7-Офис.

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), 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;
- 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.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению подготовки (специальности) 09.03.02 «Информационные системы и технологии».

Составитель(и):

доцент Гулевич Тамара Михайловна (кафедра автоматизации и информационных систем);

доцент Добрынин Алексей Сергеевич (кафедра автоматизации и информационных систем).

Рабочая программа дисциплины рассмотрена и утверждена на заседании кафедры.

Приложение

Аннотация

рабочей программы дисциплины «Информационная безопасность и защита информации»

по направлению подготовки (специальности)

09.03.02 «Информационные системы и технологии»

(направленность (профиль): «Информационные системы и технологии»)

форма обучения – Заочная форма

1 Цели и задачи освоения учебной дисциплины

Целями учебной дисциплины являются:

- изучение теоретических и прикладных аспектов информационной безопасности;
- знакомство с базовыми технологиями защиты информации в информационных системах.

Задачами учебной дисциплины являются:

- изучение типовых механизмов обеспечения безопасности информационных систем;
- получение навыков использования криптографических средств защиты данных в приложениях.

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

Учебная дисциплина относится к учебным дисциплинам обязательной части **Блока 1 «Дисциплины (модули)»** ООП по направлению подготовки (специальности) 09.03.02 «Информационные системы и технологии».

Учебная дисциплина базируется на предварительном усвоении обучающимися учебных дисциплин:

- Математика;
- Информатика;
- Основы программирования;
- Технологии программирования.

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

- Проектирование информационно-управляющих систем;
- Программное обеспечение информационно-управляющих систем.

3 Планируемые результаты обучения по учебной дисциплине

Процесс изучения учебной дисциплины направлен на формирование следующих компетенций:

– Общепрофессиональные компетенции

Наименование категории (группы) ОПК	Код и наименование ОПК	Код и наименование индикатора достижения ОПК	Планируемые результаты обучения
	ОПК-2: Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности	ОПК-2.3 Применяет современные информационные технологии и программные средства при решении прикладных задач	<p>– знать: информационные технологии и программные средства обеспечения информационной безопасности.</p> <p>– уметь: проектировать многоуровневые системы защиты информации.</p>
	ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.2 Понимает и использует принципы защиты информации и обеспечивает информационную безопасность	<p>– знать: методы, подходы и принципы защиты данных в информационных системах.</p> <p>– уметь: проектировать и реализовывать прикладные решения в области защиты данных.</p>

4 Объем учебной дисциплины

Сессия / курс		ИТОГО	2 сессия / 4 курс	3 сессия / 4 курс
Форма промежуточной аттестации				<i>экзамен</i>
Трудоёмкость	<i>академ. час.</i>	144	36	108
	<i>зачетных единиц</i>	4	1	3
Лекции, <i>академ. час.</i>		2	2	0
в форме практической подготовки		0	0	0
Лабораторные работы, <i>академ. час.</i>		0	0	0
в форме практической подготовки		0	0	0
Практические занятия, <i>академ. час.</i>		2	0	2
в форме практической подготовки		0	0	0

Курсовая работа / проект, <i>академ. час.</i>	0	0	0
в форме практической подготовки	0	0	0
Консультации, <i>академ. час.</i>	0	0	0
в форме практической подготовки	0	0	0
Самостоятельная работа, <i>академ. час.</i>	131	34	97
в форме практической подготовки	0	0	0
Контроль, <i>академ. час.</i>	9	0	9
в форме практической подготовки	0	0	0

5 Краткое содержание учебной дисциплины

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

Раздел 1 Информационная безопасность;

Тема 1.1 Термины и определения (понятия информационной безопасности, конфиденциальность, целостность, доступность, уязвимость, комплексная защита, риски);

Тема 1.2 Типовые проблемы безопасности (типовые уязвимости информационных систем, phishing - атаки, spoofing атаки, poisoning - атаки, сетевой флуд, arp, ip spoofing (poisoning), отказ в обслуживании);

Тема 1.3 Безопасность программного обеспечения (атаки на программное обеспечение, внедрение внешнего кода, атаки crossscripting и injection (SQL injection), переполнение буфера, атаки переполнения буфера, принципы безопасного программирования);

Раздел 2 Элементы криптографии;

Тема 2.1 Введение в криптографию (история криптографии, логические и криптозащиты (защиты Кирхгофа), перестановочные, подстановочные шифры, примеры логических защит);

Тема 2.2 симметричная криптография (криптозащиты, блочные и поточные схемы шифрования, принципы реализации блочных и поточных защит с закрытым ключом, схема Фейстеля, алгоритмы Triple DES, Rijndael (AES));

Тема 2.3 односторонние хэш функции (задачи хэширования данных, контрольные суммы, односторонние хэш функции, алгоритмы md5, sha1);

Тема 2.4 асимметричная криптография (идея открытого ключа, простые числа и преобразования, алгоритм RSA (Rivest, Shamir, Adelman), протокол Диффи - Хеллмана);

Тема 2.5 электронная цифровая подпись (идея электронной цифровой подписи, цифровые сертификаты, схемы с посредником, алгоритмы RSA, DSA в системах с цифровой подписью);

Тема 2.6 аутентификация и авторизация (системы аутентификации и авторизации, задачи, технологии, реализация подсистем аутентификации и авторизации).

6 Составитель(и):

доцент Гулевич Тамара Михайловна (кафедра автоматизации и информационных систем);

доцент Добрынин Алексей Сергеевич (кафедра автоматизации и информационных систем).