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
Очная форма

Срок обучения: 4 года

Год начала подготовки 2023

Новокузнецк
2023

СибГИУ
Подлинник электронного документа хранится в системе электронного согласования документов СибГИУ
ДОКУМЕНТ ПОДПИСАН ЭП
Сертификат: 861a8d56fc2cfb6de53bd665403c592fd02b1419
Владелец: Ректор Юрьев Алексей Борисович
Действителен: с 12 февраля 2024 г. по 7 мая 2025 г.
Дата и время: 01-03-2024 01:44:34 ПРОВЕРИТЬ ПОДПИСЬ

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, умения и навыки, получаемые по одновременно изучаемым и последующим 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. – владеть: навыками анализа защищенности информационных систем.
	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. – владеть: прикладными инструментальными средствами 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, лабораторные работы, коллоквиумы), 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***	***7 семестр***
Форма промежуточной аттестации			*экзамен*
Трудоёмкость	*академ. час.*	***144***	*144*

зачетных единиц		***4***	*4*
Лекции, *академ. час.*		***16***	*16*
в форме практической подготовки		***0***	*0*
Лабораторные работы, *академ. час.*		***16***	*16*
в форме практической подготовки		***0***	*0*
Практические занятия, *академ. час.*		***16***	*16*
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.*		***60***	*60*
в форме практической подготовки		***0***	*0*
Контроль, *академ. час.*		***36***	*36*
в форме практической подготовки		***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 crosscripting 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, *академ.час*	
		всего	**в форме практической подготовки**
Раздел 1.	Информационная безопасность		
Тема 1.1.	Термины и определения	1	
Тема 1.2.	Типовые проблемы безопасности	2	
Тема 1.3.	Безопасность программного обеспечения	2	
Раздел 2.	Элементы криптографии		
Тема 2.1.	Введение в криптографию	2	
Тема 2.2.	симметричная криптография	2	
Тема 2.3.	односторонние хэш функции	2	
Тема 2.4.	асимметричная криптография	2	
Тема 2.5.	электронная цифровая подпись	2	
Тема 2.6.	аутентификация и авторизация	1	
Итого:		**16**	**0**

6 Перечень тем практических занятий (семинаров)

№ раздела / темы дисциплины	Темы практических занятий (семинаров)	Трудоемкость, *академ.час*	
		всего	**в форме практической подготовки**
Тема 1.1.	Использование инструментов анализа и мониторинга сетевого трафика. Cisco packet tracer, wireshark, nmap. Анализ сетевого трафика.	1	
Тема 1.2.	Инструментарий статического анализа исходного кода. Безопасность кода. Рекомендации по безопасному программированию.	1	

Тема 1.3.	Уязвимости программного обеспечения. Переполнение буфера. Внедрение SQL. Реализация атак на переполнение буфера и внедрение SQL.	2	
Тема 2.1.	Логическая защита. Реализация логических защит. Алфавитная замена, подстановочные и перестановочные шифры. Программная реализация логических защит.	2	
Тема 2.2.	Криптозащиты. Блочные и поточные алгоритмы шифрования. Симметричные алгоритмы. Идея закрытого ключа. Вектор инициализации. Схема Фейстеля. Алгоритм Triple DES. Алгоритм rijndael (AES). Программная реализация DES, AES. Стандарт IDEA.	2	
Тема 2.3.	Криптозащиты. Односторонние хэш функции. Вычисление контрольной суммы. Алгоритмы md5, sha1. Вычисление хэш последовательности.	2	
Тема 2.4.	Криптозащиты. Идея открытого ключа. Асимметричные алгоритмы. Протокол Диффи-Хэллмана. Генерация простых чисел. Идея алгоритма RSA (Rivest, Shamir, Adelman). Программная реализация RSA.	2	
Тема 2.5.	Криптозащиты. Электронная цифровая подпись. Идея электронной цифровой подписи. Алгоритмы RSA, DSA в задачах цифровой подписи. Программная реализация DSA.	2	
Тема 2.6.	Аутентификация. Ресурсно - ролевые модели	2	

	аутентификации. Реализация ресурсно - ролевой модели аутентификации		
Итого:		**16**	**0**

7 Перечень тем лабораторных работ

№ раздела / темы дисциплины	**Темы лабораторных работ**	**Трудоемкость, *академ.час***	
		всего	**в форме практической подготовки**
Тема 2.1.	Реализация подсистемы криптографической защиты информации на основе файлового хранения	4	
Тема 2.2.	Реализация подсистемы криптографической защиты данных в сети	4	
Тема 2.3.	Реализация подсистемы электронной цифровой подписи данных	4	
Тема 2.4.	Механизмы распределенной аутентификации	4	
Итого:		**16**	**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. Оформление отчета о практической работе; 3. Подготовка к практическому занятию; 4. Прохождение тестирования.	20	

Раздел 2.	1. Изучение лекционного материала; 2. Оформление отчета о практической работе; 3. Оформление отчета по лабораторной работе; 4. Подготовка к лабораторной работе; 5. Подготовка к практическому занятию; 6. Прохождение тестирования.	40	
Контроль	*Подготовка к экзамену*	36	
Итого:		**96**	**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: 29.07.2023);

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: 29.07.2023);

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: 29.07.2023).

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:

– 7-Zip;

– Adobe Acrobat Reader;

– Astra Linux Special Edition.

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 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 – Очная 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, умения и навыки, получаемые по одновременно изучаемым и последующим 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	– знать: информационные технологии и программные средства обеспечения информационной безопасности. – уметь: проектировать многоуровневые системы защиты информации. – владеть: навыками анализа защищенности информационных систем.
	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. – владеть: прикладными инструментальными средствами защиты данных.

4 Объем учебной дисциплины

Семестр / курс		*ИТОГО*	***7 семестр***
Форма промежуточной аттестации			*экзамен*
Трудоёмкость	*академ. час.*	***144***	*144*
	зачетных единиц	***4***	*4*
Лекции, *академ. час.*		***16***	*16*
в форме практической подготовки		***0***	*0*
Лабораторные работы, *академ. час.*		***16***	*16*
в форме практической подготовки		***0***	*0*
Практические занятия, *академ. час.*		***16***	*16*

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.*	***60***	*60*
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 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 crosscripting 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 Добрынин Алексей Сергеевич (кафедра автоматизации и информационных систем).