МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Филиал КузГТУ в г. Новокузнецке

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 65A182AF55E85519218FE36C1C7FB48A
Владелец: Евсина Татьяна Алексеевна
Действителен: с 16.11.2022 до 09.02.2024

УТВЕРЖДЕНО
Директор филиала
КузГТУ в г. Новокузнецке
_____ Т.А. Евсина
«___»_____ 2023

Рабочая программа дисциплины

Информационная безопасность

Направление подготовки 09.03.03 Прикладная информатика
Направленность (профиль) 01 Прикладная информатика в экономике

Присваиваемая квалификация
«Бакалавр»

Формы обучения
очная

Год набора 2023

Новокузнецк 2023 г.

Рабочая программа обсуждена на заседании
учебно-методического совета филиала КузГТУ
в г. Новокузнецке

Протокол № 6 от 29.05.2023

Зав. кафедрой ТДиИТ _____ А.В. Ионина
подпись

СОГЛАСОВАНО:
Заместитель директора по УР _____ Т.А. Евсина
подпись

1 Перечень планируемых результатов обучения по дисциплине "Информационная безопасность", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:

общепрофессиональных компетенций:

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-4 - Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью;

Результаты обучения по дисциплине определяются индикаторами достижения компетенций

Индикатор(ы) достижения:

Выполняет установку, настройку, эксплуатацию и поддержку в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований; способен собирать и анализировать исходные данные для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности.

Выполняет участие в разработке технологической и эксплуатационной документации.

Результаты обучения по дисциплине:

Знать основные понятия и определения информационной безопасности, источники, риски и формы атак на информацию, угрозы, которым подвергается информация.

Знать требования к защите информации определенного типа.

Уметь выявлять источники, риски и формы атак на информацию, разрабатывать политику компании в соответствии со стандартами безопасности, использовать криптографические модели, алгоритмы шифрования информации и аутентификации пользователей, составлять многоуровневую защиту корпоративных сетей.

Уметь подобрать и обеспечить защиту информации.

Владеть навыками анализа и оценки эффективности систем информационной безопасности.

Владеть современными средствами защиты информации.

2 Место дисциплины "Информационная безопасность" в структуре ОПОП бакалавриата

Для освоения дисциплины необходимы знания умения, навыки и (или) опыт профессиональной деятельности, полученные в рамках изучения следующих дисциплин: Алгоритмизация и программирование.

Дисциплина входит в Блок 1 «Дисциплины (модули)» ОПОП. Цель дисциплины - получение обучающимися знаний, умений, навыков и (или) опыта профессиональной деятельности, необходимых для формирования компетенций, указанных в пункте 1.

3 Объем дисциплины "Информационная безопасность" в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины "Информационная безопасность" составляет 6 зачетных единиц, 216 часов.

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
Курс 3/Семестр 6			
Всего часов	216		
Контактная работа обучающихся с преподавателем (по видам учебных занятий):			
Аудиторная работа			

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
Лекции	16		
Лабораторные занятия	32		
Практические занятия			
Внеаудиторная работа			
Индивидуальная работа с преподавателем:			
Консультация и иные виды учебной деятельности			
Самостоятельная работа	132		
Форма промежуточной аттестации	экзамен /36		

4 Содержание дисциплины "Информационная безопасность", структурированное по разделам (темам)

4.1. Лекционные занятия

Раздел дисциплины, темы лекций и их содержание	Трудоемкость в часах		
	ОФ	ЗФ	ОЗФ
Введение в криптографию. История криптографии и криптоанализа, простейшие исторические шифры и их свойства, композиции шифров, блочные и потоковые шифры, понятие симметричных и ассиметричных криптосистем	2		
Математические основы криптографии. Понятие сложности алгоритма, алгоритм быстрого возведения в степень, обобщенный алгоритм Евклида. Модулярная арифметика. Линейные сравнения. Системы линейных сравнений. Методы получения случайных и псевдослучайных последовательностей	2		
Симметричные криптосистемы. Шифры замены, перестановки. Блочные шифры: проблема выравнивания, требования к по-строению блочных шифров. Сети Файстеля (на примере DES). Подстановочноперестановочные сети (на примере AES).Поточные шифры: синтез поточных шифров, требования к поточным шифрам. Режимы шифрования, особенности практического применения симметричных алгоритмов шифрования	4		
Ассимметричные криптосистемы. Схема открытого распределения ключей Диффи-Хеллмана. Алгоритм RSA. Криптосистема Рабина. Криптосистема Эль-Гамаля. Гибридные криптосистемы.	4		
Криптографические средства контроля целостности. Симметричные и ассимметричные средства контроля целостности. Функции хеширования.Электронная цифровая подпись. Цифровая подпись на основе RSA, криптосистемы Рабина и Эль Гамаля. Существующие уязвимости ЭЦП учебных версий криптосистем RSA, Рабина и ЭльГамаля.	4		
Итого	**16**		

4.2. Лабораторные занятия

Наименование работы	Трудоемкость в часах		
	ОФ	ЗФ	ОЗФ

Ознакомиться с классическими симметричными криптосистемами, реализовать шифр Цезаря, шифр Виженера, шифр Скиталы.	6		
Познакомиться с основными методами генерации случайных больших простых чисел	8		
Изучение современного алгоритма блочного шифрования AES. Анализ его структуры и упрощенная реализация.	8		
Ознакомиться с основами дифференциального криптоанализа на примере стандарта шифрования DES. Собственная реализация алгоритма.	10		
Итого	**32**		

4.3 Практические (семинарские) занятия

Тема занятия	Трудоемкость в часах		
	ОФ	ЗФ	ОЗФ
Не предусмотрены			

4.4 Самостоятельная работа обучающегося и перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Вид СРС	Трудоемкость в часах		
	ОФ	ЗФ	ОЗФ
Изучение алгоритмов шифрования.	34		
Выполнение лабораторных работ на выбранном языке программирования.	92		
Подготовка к промежеточной аттестации	6		
Итого	**132**		
Экзамен	36		

4.5 Курсовое проектирование

Не предусмотрено.

5 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине "Информационная безопасность"

5.1 Паспорт фонда оценочных средств

Планируемые результаты обучения по дисциплине (модулю)
Дисциплина направлена на формирование следующих компетенций выпускника:

Форма(ы) текущего контроля	**Компетенции, формируемые в результате освоения дисциплины (модуля)**	**Индикатор(ы) достижения**	**Результаты обучения по дисциплине (модулю)**	Уровень

Защита лабораторных работ	ОПК-3	Выполняет установку, настройку, эксплуатацию и поддержку в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований; способен собирать и анализировать исходные данные для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности.	Знать основные понятия и определения информационной безопасности, источники, риски и формы атак на информацию, угрозы, которым подвергается информация. Уметь выявлять источники, риски и формы атак на информацию, разрабатывать политику компании в соответствии со стандартами безопасности, использовать криптографические модели, алгоритмы шифрования информации и аутентификации пользователей, составлять многоуровневую защиту корпоративных сетей. Владеть навыками анализа и оценки эффективности систем информационной безопасности.	Высокий или средний
Защита лабораторных работ	ОПК-4	Выполняет участие в разработке технологической и эксплуатационной документации.	Знать требования к защите информации определенного типа. Уметь подобрать и обеспечить защиту информации. Владеть современными средствами защиты информации.	Высокий или средний
Высокий уровень достижения компетенции - компетенция сформирована, рекомендованные оценки: отлично, хорошо, зачтено. **Средний уровень достижения компетенции** - компетенция сформирована, рекомендованные оценки: хорошо, удовлетворительно, зачтено. **Низкий уровень достижения компетенции** - компетенция не сформирована, оценивается неудовлетворительно или не зачтено				

5.2. Контрольные задания или иные материалы

Текущий контроль успеваемости и аттестационные испытания обучающихся могут быть организованы с использованием ресурсов ЭИОС КузГТУ. Полный перечень оценочных материалов расположен в ЭИОС КузГТУ.: https://el.kuzstu.ru/login/index.php.

Текущий контроль успеваемости и аттестационные испытания могут проводиться в письменной и (или) устной, и (или) электронной форме.

5.2.1.Оценочные средства при текущем контроле

Текущий контроль по дисциплине будет заключаться в защите обучающимися выполненных лабораторных работ.

На защите преподавателем будет задано 2-4 вопроса в соответствии с тематикой лабораторной работы.

Например:

1. Что такое симметриченые алгоритмы.
2. Для чего нужен алгоритм Евклида.
3. Особенности асиметричных алгоритмов.
4. Что такое ключ шифра.
5. Особенности алгоритма RSA.

Количество баллов	0-74	75-100
Шкала оценивания	Не зачтено	Зачтено

5.2.2 Оценочные средства при промежуточной аттестации

Формой промежуточной аттестации является экзамен, в процессе которого определяется сформированность обозначенных в рабочей программе компетенций. Инструментом измерения сформированности компетенций являются оформленные и зачтенные отчеты по лабораторным работам, ответы на вопросы во время опроса по темам лекций, экзаменационные вопросы.

На экзамене обучающийся отвечает на билет, в котором содержится 2 вопроса. Оценка за экзамен выставляется с учетом отчетов по лабораторным работам и ответа на вопросы.

Критерии оценивания:

- 100 баллов – при правильном и полном ответе на два вопроса;
- 75…99 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 50…74 баллов – при правильном и неполном ответе на два вопроса или правильном и полном ответе только на один из вопросов;
- 25…49 баллов – при правильном и неполном ответе только на один из вопросов;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-64	65-74	75-84	85-100
Шкала оценивания	Неуд.	Удовл	Хорошо	Отлично

5.2.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций

Текущий контроль успеваемости обучающихся по результатам выполнения лабораторных работ осуществляется в форме собеседования после представления обучающимся результатов выполнения лабораторной работы на электронном носителе. Научно-педагогический работник, после проведения оценочных процедур, имеет право вернуть обучающемуся работу для последующей корректировки с указанием перечня несоответствий. Обучающийся обязан устранить все указанные несоответствия и представить лабораторную научно-педагогическому работнику в срок, не превышающий трех учебных дней, следующих за днем проведения текущего контроля успеваемости.

Результаты текущего контроля доводятся до сведения обучающихся в течение трех учебных дней, следующих за днем проведения текущего контроля успеваемости.

Обучающиеся, которые не прошли текущий контроль успеваемости в установленные сроки, обязаны пройти его в срок до начала процедуры промежуточной аттестации по дисциплине в соответствии с расписанием промежуточной аттестации.

Результаты прохождения процедур текущего контроля успеваемости обучающихся учитываются при оценивании результатов промежуточной аттестации обучающихся.

До промежуточной аттестации допускается обучающийся, который выполнил все требования текущего контроля (защитил лабораторные работы).

Промежуточная аттестация обучающихся проводится после завершения обучения по дисциплине в семестре в соответствии с календарным учебным графиком и расписанием промежуточной аттестации. Процедура промежуточной аттестации описана в п. 5.2.2.

6 Учебно-методическое обеспечение

6.1 Основная литература

1. Мельников, В. П. Информационная безопасность и защита информации : учеб. пособие для студентов вузов, обучающихся по специальности "Информационные системы и технологии" / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. – 5-е изд., стер. – Москва : Академия, 2011. – 336 с. – (Высшее профессиональное образование : Информатика и вычислительная техника). – Текст : непосредственный.

2. Спицын, В. Г. Информационная безопасность вычислительной техники / В. Г. Спицын ; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск : Эль Контент, 2011. – 148 с. – ISBN 9785433200203. – URL: http://biblioclub.ru/index.php?page=book_red&id=208694 (дата обращения: 21.03.2023). – Текст : электронный.

6.2 Дополнительная литература

1. Информационная безопасность и защита информации ; Ответственный редактор: Колябин А. Ю.. – Москва : Студенческая наука, 2012. – 1322 с. – ISBN 9785000461372. – URL: http://biblioclub.ru/index.php?page=book_red&id=227774 (дата обращения: 21.03.2023). – Текст : электронный.

2. Бурова, М. А. Информационная безопасность и защита информации : учебное пособие / М. А. Бурова, А. С. Овсянников. — Самара : СамГУПС, [б. г.]. — Часть 2 — 2012. — 150 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/130272 (дата обращения: 21.03.2023). — Режим доступа: для авториз. пользователей.

3. Бурова, М. А. Информационная безопасность и криптографическая защита информации : учебное пособие / М. А. Бурова. — Самара : СамГУПС, 2009. — 98 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/130271 (дата обращения: 21.03.2023). — Режим доступа: для авториз. пользователей.

6.3 Методическая литература

6.4 Профессиональные базы данных и информационные справочные системы

1. Электронная библиотечная система «Университетская библиотека онлайн» http://biblioclub.ru/
2. Электронная библиотечная система «Лань» http://e.lanbook.com
3. Электронная библиотека КузГТУ https://elib.kuzstu.ru/index.php?option=com_content&view=article&id=230&Itemid=229

6.5 Периодические издания

1. Информация и безопасность : научный журнал (печатный)

7 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

ЭИОС КузГТУ:

a) Электронная библиотека КузГТУ. – Текст: электронный // Научно-техническая библиотека Кузбасского государственного технического университета им. Т. Ф. Горбачева : сайт. – Кемерово, 2001 – . – URL: https://elib.kuzstu.ru/. – Текст: электронный.

b) Портал.КузГТУ : Автоматизированная Информационная Система (АИС) : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://portal.kuzstu.ru/. – Режим доступа: для авториз. пользователей. – Текст: электронный.

c) Электронное обучение : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://el.kuzstu.ru/. – Режим доступа: для авториз. пользователей КузГТУ. – Текст: электронный.

8 Методические указания для обучающихся по освоению дисциплины "Информационная безопасность"

Самостоятельная работа обучающегося является частью его учебной деятельности, объемы самостоятельной работы по каждой дисциплине (модулю) практике, государственной итоговой аттестации, устанавливаются в учебном плане.

Самостоятельная работа по дисциплине (модулю), практике организуется следующим образом:

1. До начала освоения дисциплины обучающемуся необходимо ознакомиться с содержанием рабочей программы дисциплины (модуля), программы практики в следующем порядке:

1.1 содержание знаний, умений, навыков и (или) опыта профессиональной деятельности, которые будут сформированы в процессе освоения дисциплины (модуля), практики;

1.2 содержание конспектов лекций, размещенных в электронной информационной среде КузГТУ в порядке освоения дисциплины, указанном в рабочей программе дисциплины (модуля), практики;

1.3 содержание основной и дополнительной литературы.

2. В период освоения дисциплины обучающийся осуществляет самостоятельную работу в следующем порядке:

2.1 выполнение практических и (или) лабораторных работы и (или) отчетов в порядке, установленном в рабочей программе дисциплины (модуля), практики;

2.2 подготовка к опросам и (или) тестированию в соответствии с порядком, установленном в рабочей программе дисциплины (модуля), практики;

2.3 подготовка к промежуточной аттестации в соответствии с порядком, установленном в рабочей программе дисциплины (модуля), практики.

В случае затруднений, возникших при выполнении самостоятельной работы, обучающемуся необходимо обратиться за консультацией к педагогическому работнику. Периоды проведения консультаций устанавливаются в расписании консультаций.

9 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине "Информационная безопасность", включая перечень программного обеспечения и информационных справочных систем

Для изучения дисциплины может использоваться следующее программное обеспечение:

1. Mozilla Firefox
2. Google Chrome
3. Opera
4. Yandex
5. 7-zip
6. Open Office
7. Microsoft Windows
8. ESET NOD32 Smart Security Business Edition
9. Kaspersky Endpoint Security
10. Браузер Спутник

10 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине "Информационная безопасность"

Для реализации программы учебной дисциплины предусмотрены специальные помещения:

1. Помещения для самостоятельной работы обучающихся должны оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа к электронной информационно-образовательной среде Организации.

2. Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

11 Иные сведения и (или) материалы

1. Образовательный процесс осуществляется с использованием как традиционных так и современных интерактивных технологий.

В рамках аудиторных занятий применяются следующие интерактивные методы:

 разбор конкретных примеров;
 мультимедийная презентация.

2. Проведение групповых и индивидуальных консультаций осуществляется в соответствии с расписанием консультаций по темам, заявленным в рабочей программе дисциплины, в период освоения дисциплины и перед промежуточной аттестацией с учетом результатов текущего контроля.