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

Филиал КузГТУ в г. Новокузнецке

Евсина Татьяна Алексеевна

Подписан: Евсина Татьяна Алексеевна
DN: C=RU, S=Кемеровская область, L=Новокузнецк, T=Заместитель директора по УР, O="ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ ""КУЗБАССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ Т.Ф. ГОРБАЧЕВА""", СНИЛС=05710607537, ИНН=422206411361, E=director@kuzstu-nf.ru, G=Татьяна Алексеевна, SN=Евсина, CN=Евсина Татьяна Алексеевна
Основание: я подтверждаю этот документ своей удостоверяющей подписью

УТВЕРЖДЕНО
Директор филиала
КузГТУ в г. Новокузнецке
_____ Т.А. Евсина
«28» _____ 2024

**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 2024

Новокузнецк 2024 г.

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

Протокол № 6 от 29.05.2024

Зав. кафедрой ИТиЭД  В.В. Шарлай

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 | | | |
| *Лекции* | 16 | | |
| *Лабораторные занятия* | 32 | | |
| *Практические занятия* | | | |

| Форма обучения | Количество часов | | |
|---|---|---|---|
| | ОФ | ЗФ | ОЗФ |
| 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.

## 6 Учебно-методическое обеспечение

### 6.1 Основная литература

1. Прохорова, О. В. Информационная безопасность и защита информации : учебник : [16+] / О. В. Прохорова ; Самарский государственный архитектурно-строительный университет. – Самара : Самарский государственный архитектурно-строительный университет, 2014. – 113 с. : табл., схем., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=438331 (дата обращения: 05.06.2022). – ISBN 978-5-9585-0603-3. – Текст : электронный

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: 05.06.2022). – 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: 13.09.2020). – 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: 01.04.2022). — 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: 01.04.2022). — 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://library.kuzstu.ru/index.php/punkt-18

### 6.5 Периодические издания

1. Информация и безопасность : научный журнал (электронный)
https://elibrary.ru/title_about_new.asp?id=8748

## 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://library.kuzstu.ru/index.php/punkt-2/ebs. – 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.