МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«КУЗБАССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ Т.Ф.ГОРБАЧЕВА»
Филиал КузГТУ в г. Белово

УТВЕРЖДАЮ

Директор филиала
КузГТУ в г. Белово
И.К. Костинец

Подписано цифровой подписью: Костинец Ирина Константиновна
DN: cn=Костинец Ирина Константиновна, o=Кузбасский государственный технический университет имени Т.Ф.Горбачева, ou=филиал КузГТУ в г.Белово, email=kostinets@yandex.ru, c=RU
Дата: 2023.06.13 08:31:55 +07'00'

Рабочая программа дисциплины

Информационная безопасность

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

Присваиваемая квалификация
"Бакалавр"

Форма обучения очная

год набора 2021

Белово 2023

Рабочую программу составил: старший преподаватель Аксененко Е.Г.

Рабочая программа обсуждена на заседании кафедры «Экономики и информационных технологий»
Протокол № 10 от «13» мая 2023 г.
Заведующий кафедрой: Верчагина И.Ю.

Верчагина Ирина Юрьевна

Подписано цифровой подписью: Верчагина Ирина Юрьевна
DN: cn=Верчагина Ирина Юрьевна, o=филиал КузГТУ в г.Белово, ou=кафедра экономики и информационных дисциплин, email=viy.77@mail.ru, c=RU
Дата: 2023.05.24 13:56:40 +07'00'

Согласовано учебно-методической комиссией по направлению подготовки 09.03.03 «Прикладная информатика»
Протокол № 9 от «16» мая 2023 г.
Председатель комиссии: Колечкина И.П.

Колечкина Ирина Павловна

Подписано цифровой подписью: Колечкина Ирина Павловна
DN: cn=Колечкина Ирина Павловна, o=Филиал КузГТУ в г.Белово, ou=Кафедра экономики и информационных технологий, email=40882kip@mail.ru, c=RU
Дата: 2023.06.01 11:48:05 +07'00'

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;
- 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;
- подобрать и обеспечить защиту информации навыками анализа и оценки эффективности систем информационной безопасности.

Владеть:

- навыками анализа и оценки эффективности систем информационной безопасности;
- 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			
Внеаудиторная работа			
Индивидуальная работа с преподавателем:			
Консультация и иные виды учебной деятельности			
Самостоятельная работа	132		
Форма промежуточной аттестации	экзамен		

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 построению блочных шифров. Сети Файстеля (на примере DES) . Подстановочно-перестановочные 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 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		

5 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине "Информационная безопасность", структурированное по разделам (темам)

5.1 Паспорт фонда оценочных средств

Форма(ы) текущего контроля	Компетенции, формируемые в результате освоения дисциплины (модуля)	Индикатор(ы) достижения компетенции	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 навыками анализа и оценки эффективности систем информационной безопасности. Владеть: - современными средствами защиты информации.	Высокий или средний
Высокий уровень результатов обучения – знания, умения и навыки соотносятся с индикаторами достижения компетенции, рекомендованные оценки: отлично; хорошо; зачтено. **Средний уровень результатов обучения** – знания, умения и навыки соотносятся с индикаторами достижения компетенции, рекомендованные оценки: хорошо; удовлетворительно; зачтено. **Низкий уровень результатов обучения** – знания, умения и навыки не соотносятся с индикаторами достижения компетенции, оценивается неудовлетворительно или не зачтено.				

5.2 Типовые контрольные задания или иные материалы

Текущий контроль успеваемости и промежуточная аттестация обучающихся могут проводиться как при непосредственном взаимодействии педагогического работника с обучающимися, так и с использованием ресурсов ЭИОС филиала КузГТУ, в том числе синхронного и (или) асинхронного взаимодействия посредством сети «Интернет».

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 симметричные алгоритмы.

2.Для чего нужен алгоритм Евклида.

3.Особенности ассиметричных алгоритмов.

4.Что такое ключ шифра.
5.Особенности алгоритма RSA.

Критерии оценивания

- 90–100 баллов – при правильном выполнении заданий лабораторной работы, правильном ответе на все заданные вопросы;
- 80–89 баллов – при правильном выполнении заданий лабораторной работы, недостаточно полных ответов на заданные вопросы;
- 60–79 баллов – при неполном выполнении заданий лабораторной работы и/или неправильных, неточных ответах на вопросы;
- 0–59 баллов – при наличии серьезных ошибок при выполнении заданий лабораторной работы, неправильных ответах на вопросы или отсутствии выполненного задания и/или ответов на вопросы.

Шкала оценивания

Количество баллов	0–59	60–79	80-89	90-100
Шкала оценивания	Неудовлетворительно	Удовлетворительно	Хорошо	Отлично
	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	0–59	60–79	80-89	90-100
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. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2023. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/519780.

2. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2023. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/520063.
3. Прохорова, О. В. Информационная безопасность и защита информации / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург : Лань, 2023. — 124 с. — ISBN 978-5-507-46010-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/293009. — Режим доступа: для авториз. пользователей..

6.2. Дополнительная литература

1. Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/165837. — Режим доступа: для авториз. пользователей.
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. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511239.
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. — Режим доступа: для авториз. пользователей.
4. 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. — Режим доступа: для авториз. пользователей..

6.3 Профессиональные базы данных и информационные справочные системы

1. Электронная библиотека КузГТУ https://elib.kuzstu.ru/
2. Электронная библиотечная система «Лань» http://e.lanbook.com
3. Электронная библиотечная система Новосибирского государственного технического университета https://clck.ru/UoXpv
4. Электронная библиотечная система «Юрайт» https://urait.ru/

6.4 Периодические издания

1. Информационное общество. Научно-аналитический журнал [Электронный ресурс]. - Режим доступа: http://infosoc.iis.ru.

7 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Официальный сайт Кузбасского государственного технического университета имени Т.Ф. Горбачева. Режим доступа: https://kuzstu.ru/.
2. Официальный сайт филиала КузГТУ в г. Белово. Режим доступа: http://belovokyzgty.ru/.
3. Электронная информационно-образовательная среда филиала КузГТУ в г. Белово. Режим доступа: http://eos.belovokyzgty.ru/
4. Научная электронная библиотека eLIBRARY.RU https://elibrary.ru/defaultx.asp?

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 филиала 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. Open Office
6. Microsoft Windows
7. ESET NOD32 Smart Security Business Edition

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

Для осуществления образовательного процесса по дисциплине предусмотрены специальные помещения:

Помещение № 209 (компьютерный класс) представляет собой учебную аудиторию для проведения учебных занятий, предусмотренных программой бакалавриата, оснащенную оборудованием и техническими средствами обучения

Перечень основного оборудования:

Автоматизированные рабочие места -12

Автоматизированное рабочее место преподавателя.

Процессор Intel Core i3-2120 Sandy Bridge 3300 МГц

Оперативная память 8 Гб, жёсткий диск 512 Гб 7200 rpm, видеокарта NVIDIA GeForce GT 710 1 Гб

Проектор Benq MX с максимальным разрешением 1024x768.

Проекционный экран

Многофункциональное устройство формата А4

Маркерная доска

Специализированная мебель

Учебно-наглядные пособия:

Тематические иллюстрации.

Программное обеспечение:

Операционная система Microsoft Windows 10

Пакеты программных продуктов Office 2010.

Средство антивирусной защиты ESET Endpoint Antivirus

Eclipse IDE for Java EE Developers, NET Framework JDK 8, Microsoft SQL Server Express Edition, Microsoft Visio Professional, My SQL Installer for Windows, Net Beans, SQL Server Management Studio, Microsoft SQL Server Java Connector, Android Studio, IntelliJ IDEA, nanoCAD САПР для инженеров, Math CAD, AutoCAD 2015

Помещение № 219 для самостоятельной работы обучающихся оснащенное компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронно-образовательную среду Организации.

Перечень основного оборудования:

Автоматизированные рабочие места – 10

Компьютер-моноблок Lenovo Idea Centre C225 -10 шт.

Диагональ18.5"Разрешение1366 x 768

Типовая конфигурация AMDE-Series / 1.7 ГГц / 2 Гб / 500 Гб

Гигабитный Ethernet

Максимальный объем оперативной памяти 8Гб

ИнтерфейсыRJ-45иHDMI.

Учебная мебель

Учебно-наглядные пособия:

Информационные стенды 2 шт.

Тематические иллюстрации.

Программное обеспечение:

Операционная система Microsoft Windows10

Пакеты программных продуктов Office 2010.

Средство антивирусной защиты ESET Endpoint Antivirus

Доступ к электронным библиотечным системам «Лань», «Юрайт», «Технорматив», электронной библиотеке КузГТУ, справочно - правовой системе «КонсультантПлюс», электронной информационно-образовательной среде филиала КузГТУ в г. Белово, информационно-коммуникационной сети «Интернет».

АБИС: 1-С библиотека.

Помещение № 318 для самостоятельной работы обучающихся оснащенное компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронно-образовательную среду Организации.

Перечень основного оборудования:

Общая локальная компьютерная сеть Интернет.
Автоматизированные рабочие места – 20
Ноутбуки-20
Автоматизированное рабочее место преподавателя
Процессор Intel Core i3-2120 Sandy Bridge 3300 МГц s1155, оперативная память 8 Гб (2x4 Гб) DDR3 1600МГц, жёсткий диск 500 Гб 7200 rpm
Видео-карта AMD Radeon RX 560 2 Гб
Принтер лазерный HP LaserJet Pro M104a
Интерактивная система SmartBoardSB680
Переносная кафедра
Флипчарт
Учебная мебель

Учебно-наглядные пособия:

Перекидные системы – 2шт.
Тематические иллюстрации

Программное обеспечение:

Операционная система Microsoft Windows 10
Пакеты программных продуктов Office 2010.
Средство антивирусной защиты ESET Endpoint Antivirus
Программный комплекс Smart для интерактивных комплектов.

Доступ к электронным библиотечным системам «Лань», «Юрайт», «Академия», «Znanium,com» электронной библиотеке КузГТУ, электронной информационно-образовательной среде филиала КузГТУ в г. Белово, информационно-коммуникационной сети «Интернет».

11 Иные сведения и (или) материалы

При осуществлении образовательного процесса применяются следующие образовательные технологии:

- традиционная с использованием современных технических средств;
- интерактивная.