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
_____ И.К. Костинец
«_31_»____08_____ 20_21_ г.

Подписано цифровой подписью: Долганова Жанна Александровна
DN: cn=Долганова Жанна Александровна, o=Кузбасский государственный технический университет имени Т.Ф.Горбачева, ou=Филиал КузГТУ в г.Белово, email=dolganovaja@kuzstu.ru, c=RU
Дата: 2023.11.21 11:28:34 +07'00'

Фонд оценочных средств по дисциплине

Информационная безопасность

Направление подготовки 09.03.03 «Прикладная информатика»
Профиль 01 «Прикладная информатика в экономике»

Присваиваемая квалификация "Бакалавр"

Белово 2021

ФОС составил ст. преподаватель _____ Е.Г. Аксененко

ФОС обсужден на заседании кафедры горного дела и техносферной безопасности

Протокол № _10__ от «__15_»_____06____ 2021 г.

Зав. кафедрой горного дела и техносферной безопасности _____ В.Ф. Белов

Согласовано учебно-методическим советом филиала КузГТУ в г. Белово

Протокол № __11___ от «_22___»___06_____ 2021 г.

Председатель учебно-методического совета _____ Ж.А. Долганова

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

Освоение дисциплины направлено на формирование:

общепрофессиональных компетенций:

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

ОПК-6 - Способен анализировать и разрабатывать организационно-технические и экономические процессы с применением методов системного анализа и математического моделирования.

ОПК-8 - Способен принимать участие в управлении проектами создания информационных систем на стадиях жизненного цикла.

ОПК-9 - Способен принимать участие в реализации профессиональных коммуникаций с заинтересованными участниками проектной деятельности и в рамках проектных групп.

универсальных компетенций:

УК-1 - Способен осуществлять поиск, критический анализ и синтез информации, применять системный

Результаты обучения по дисциплине определяются индикаторами достижения компетенций

Индикатор(ы) достижения:

Владеет основами поиска информации в библиографических источниках и в сети Интернет, критического анализа и синтеза информации, системного подхода при решении поставленных задач; принципами сбора, отбора и обобщения информации.

Владеет стандартами оформления технической документации на различных стадиях жизненного цикла информационной системы.

Владеет методами теории систем и системного анализа, математического и имитационного моделирования для автоматизации задач принятия решений, анализа информационных потоков, расчета экономической эффективности и надежности информационных систем и технологий.

Владеет навыками составления плановой и отчетной документации по управлению проектами создания информационных систем на стадиях жизненного цикла.

Знает инструменты, методы и каналы коммуникаций в проектах; технологии межличностной и групповой коммуникации в деловом взаимодействии, технологии подготовки и проведения презентаций.

Владеет навыками проведения презентаций, переговоров, публичных выступлений.

Результаты обучения по дисциплине:

Знает:

Методы анализа прикладной области, информационных потребностей, формирования требований к ИС, методологии и технологии проектирования ИС, проектирование обеспечивающих подсистем ИС;

Методы и средства организации и управления проектом ИС на всех стадиях жизненного цикла, основы менеджмента качества ИС, методы управления IT-проектами;

Организационно-технические и экономические процессы, методы системного анализа и математического моделирования;

Примерный комплекс документов, регламентирующих деятельность персонала информационных служб в условиях функционирования информационных систем (взаимодействие работников управленческих служб и персонала информационных служб с техническими средствами и между собой);

Стадии жизненного цикла ИС

Методологии выявления реальных потребностей заказчика, типологии ролей заказчика, алгоритмы взаимодействия с различными типами заказчика.

Умеет:

Проводить анализ предметной области, выявлять информационные потребности и разрабатывать требования к ИС, проводить сравнительный анализ и выбор для решения прикладных задач и создания ИС.

Разрабатывать концептуальную модель прикладной области, выбирать инструментальные средства и технологии проектирования ИС, проводить формализацию и реализацию решения прикладных задач выполнять работы на всех стадиях жизненного цикла проекта ИС.

Анализировать и разрабатывать организационно-технические и экономические процессы.

Разрабатывать концептуальную модель прикладной области, выбирать инструментальные средства и технологии проектирования ИС, проводить формализацию и реализацию решения прикладных задач выполнять работы на всех стадиях жизненного цикла проекта ИС.

Управлять проектами создания информационных систем на различных стадиях жизненного цикла.

Проводить эффективное интервьюирование заказчиков и привлеченных к проекту профильных экспертов, формировать описание функционала проектируемой системы в терминологии принятой у заказчика.

Владеет:

Навыками работы с инструментальными средствами моделирования предметной области, прикладных и информационных процессов, способностью проектировать ИС в соответствии с профилем подготовки по видам обеспечения.

Способами разработки стандартов, норм и правил, а также технической документации.

Методами системного анализа и математического моделирования.

Способностью документировать процессы создания информационных систем на стадиях жизненного цикла.

Способами управления проектами создания информационных систем на различных стадиях жизненного цикла.

Технологиями проведения эффективных переговоров, навыками формирования ТЗ и - предпроектного исследования предметной области.

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

2.1. Паспорт фонда оценочных средств

Форма(ы) текущего контроля	Компетенции, формируемые в результате освоения дисциплины	Индикатор (ы) достижения компетенции	Результаты обучения по дисциплине (модулю)	Уровень достижения компетенции
Защита лабораторных работ	ОПК-3	Выполняет установку, настройку, эксплуатацию и поддержку в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований.	Знает: - основные понятия и определения информационной безопасности, источники, риски и формы атак на информацию, угрозы, которым подвергается информация; Умеет: - 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	Высокий или средний

		Способен собирать и анализировать исходные данные для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности.	многоуровневую защиту корпоративных сетей; Владеет: - навыками анализа и оценки эффективности систем информационной безопасности.	
Защита лабораторных работ	ОПК-4	Выполняет участие в разработке технологической и эксплуатационной документации.	Знает: - требования к защите информации определенного типа. Умеет: - подобрать и обеспечить защиту информации навыками анализа и оценки эффективности систем информационной безопасности. Владеет: - современными средствами защиты информации.	Высокий или средний
Высокий уровень достижения компетенции - компетенция сформирована частично, рекомендованные оценки: отлично, хорошо, зачтено. **Средний уровень достижения компетенции -** компетенция сформирована частично, рекомендованные оценки: хорошо, удовлетворительно, зачтено. **Низкий уровень достижения компетенции -** компетенция не сформирована частично, оценивается неудовлетворительно или не зачтено.				

2.2. 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».

2.3. Оценочные средства при текущем контроле

Текущий контроль по дисциплине будет заключаться в оформлении и защите отчетов по лабораторным работам.

Вопросы к защите лабораторных работ

1) Что такое симметричные алгоритмы?
2) Отличие симметричных и ассиметричных алгоритмов.
3) На чем основан шифр Цезаря?
4) Что такое блочные и потоковые шифры?
5) Для чего используется тест Соловея-Штрассена?
6) Как происходит шифрование в алгоритме DES?
7) В чем суть шифра Вижинера?
8) Перечислить основные характеристики алгоритма DES.
9) Для чего нужен алгоритм Евклида?
10) Алгоритм быстрого возведения в степень.

11) Особенности ассиметричных алгоритмов.
12) Что такое сеть Фейстеля?
13) В чем особенность поточного шифра?
14) В какому виду относиться алгоритм AES?
15) Сколько раундов шифрования в алгоритме DES?
16) Чему равен размер блока в DES?
17) Деление на блоки при шифровании DES.
18) Что такое ключ шифра?
19) Что такое открытый и закрытый ключ?
20) К какому типу относиться алгоритм DES и алгоритм RSA?
21) Как генерируется ключ в RSA?
22) Особенности алгоритма RSA
23) Чем определяется криптостойкость шифра?
24) Сколько ключей используется в ассиметричном алгоритме?
25) Что такое XSS уязвимость?
26) Что такое SQL инъекция?
27) Как защититься от уязвимостей?

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

<table>
<tr><td>Количество баллов</td><td>0–59</td><td>60–79</td><td>80-89</td><td>90-100</td></tr>
<tr><td rowspan="2">Шкала оценивания</td><td>Неудовлетворительно</td><td>Удовлетворительно</td><td>Хорошо</td><td>Отлично</td></tr>
<tr><td>Не зачтено</td><td colspan="3">Зачтено</td></tr>
</table>

5.2.2 Оценочные средства при промежуточной аттестации

Промежуточная аттестация проводится в форме экзамена. Экзаменационный билет включает два вопроса.

Экзаменационные вопросы

1) Современная классификация криптографических алгоритмов.
2) Блочные и потоковые шифры.
3) Шифр Цезаря.
4) Шифр скиталы.
5) Шифр Вижинера.
6) Модели нарушителя и безопасных систем. Модель Долева-Яо.
7) Шифры замены и перестановки.
8) Криптосистема Рабина.
9) Алгоритм BlowFish.
10) Криптосистема Эль-Гамаля.
11) Ddos атака и способы защиты от нее.
12) Алгоритм шифрования RC4.

13) Фишинг.
14) Схема Диффи-Хелмана.
15) Обобщенный алгоритм Евклида.
16) История криптографии и криптоанализа.
17) Подстановочно-перестановочные сети (на примере AES).
18) Алгоритм RSA.
19) Блочные и потоковые шифры.
20) Тест Соловея-Штрассена.
21) Тест Миллера-Рабина.
22) Ассиметричные алгоритмы шифрования.
23) Электронная цифровая подпись.
24) Алгоритм формирования электронной цифровой подписи.
25) Симметричные алгоритмы шифрования.
26) Современная классификация криптографических алгоритмов.
27) Схема открытого распределения ключей Диффи-Хеллмана.
28) Блочный шифр.
29) Алгоритм быстрого возведения в степень.
30) Алгоритм RSA.
31) Сети Файстеля (на примере DES).
32) Понятие и сложность алгоритма.
33) Потоковые шифры.
34) Антивирусы и антивирусные программы.
35) Шифр Вернама.
36) Основные уязвимости сайтов.
37) Алгоритм шифрования 3DES.
38) Снифферы.
39) Алгоритм шифрования DSS.
40) Алгоритм шифрования RC6.
41) Алгоритм шифрования ГОСТ 28147

Критерии оценивания:
- 90–100 баллов – при правильном и полном ответе на два вопроса;
- 80–89 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Шкала оценивания

Количество баллов	0–59	60–79	80-89	90-100
Шкала оценивания	Неудовлетворительно	Удовлетворительно	Хорошо	Отлично
	Не зачтено	Зачтено		

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

При проведении текущего контроля успеваемости в форме опроса по распоряжению педагогического работника обучающиеся убирают все личные вещи, электронные средства связи, печатные и (или) рукописные источники информации, достают чистый лист бумаги любого размера и ручку. На листе бумаги записываются Фамилия, Имя, Отчество (при наличии), номер учебной группы и дата проведения текущего контроля успеваемости. Педагогический работник

задает вопросы, которые могут быть записаны на подготовленный для ответа лист бумаги. В течение установленного педагогическим работником времени обучающиеся письменно формулируют ответы на заданные вопросы. По истечении установленного времени лист бумаги с подготовленными ответами обучающиеся передают педагогическому работнику для последующего оценивания результатов текущего контроля успеваемости.

Результаты текущего контроля успеваемости доводятся до сведения обучающихся в течение трех учебных дней, следующих за днем проведения текущего контроля успеваемости, и могут быть учтены педагогическим работником при промежуточной аттестации. Результаты промежуточной аттестации доводятся до сведения обучающихся в день проведения промежуточной аттестации. При подготовке ответов на вопросы при проведении текущего контроля успеваемости и при прохождении промежуточной аттестации обучающимся запрещается использование любых электронных средств связи, печатных и (или) рукописных источников информации. В случае обнаружения педагогическим работником факта использования обучающимся при подготовке ответов на вопросы указанных источников информации – оценка результатов текущего контроля успеваемости и (или) промежуточной аттестации соответствует 0 баллов.

При прохождении текущего контроля успеваемости и промежуточной аттестации обучающимися с ограниченными возможностями здоровья и инвалидами, допускается присутствие в помещении лиц, оказывающим таким обучающимся соответствующую помощь, а для подготовки ими ответов отводится дополнительное время с учетом особенностей их психофизического развития, индивидуальных возможностей и состояния здоровья.