МИНИСТЕРСТВО НАУКИ И ОБРАЗОВАНИЯ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Филиал КузГТУ в г. Новокузнецке

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

Фонд оценочных средств дисциплины

Информационная безопасность

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

Присваиваемая квалификация «Бакалавр»

Формы обучения очная

Год набора 2022

Новокузнецк 2023 г.

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.

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

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	0-64	65-	75-84	85-100

баллов		74		
Шкала оценивания	Неуд.	Удовл	Хорошо	Отлично

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.

Оценочные средства для формирования компетенции ОПК – 3 в процессе освоения дисциплины (модуля)

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.

Индикаторы достижения компетенции

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.

1. К правовым методам, обеспечивающим информационную безопасность, относятся:

1) Разработка аппаратных средств обеспечения правовых данных
2) Разработка и установка во всех компьютерных правовых сетях журналов учета действий
3) Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2. Основными источниками угроз информационной безопасности являются все указанное в списке:
1) Хищение жестких дисков, подключение к сети, инсайдерство
2) Перехват данных, хищение данных, изменение архитектуры системы
3) Хищение данных, подкуп системных администраторов, нарушение регламента работы

3. Виды информационной безопасности:
1) Персональная, корпоративная, государственная
2) Клиентская, серверная, сетевая
3) Локальная, глобальная, смешанная

4. Цели информационной безопасности – своевременное обнаружение, предупреждение:
1) несанкционированного доступа, воздействия в сети
2) инсайдерства в организации
3) чрезвычайных ситуаций

5. Основные объекты информационной безопасности:
1) Компьютерные сети, базы данных
2) Информационные системы, психологическое состояние пользователей
3) Бизнес-ориентированные, коммерческие системы

6. Основными рисками информационной безопасности являются:
Ответ: потеря, искажение, утечка информации

7. К основным принципам обеспечения информационной безопасности относится:
Ответ: экономической эффективности системы безопасности

8. Основными субъектами информационной безопасности являются:
Ответ: органы права, государства, бизнеса

9. К основным функциям системы безопасности можно отнести все перечисленное:
Ответ: установление регламента, аудит системы, выявление рисков

10. Принципом информационной безопасности является принцип недопущения:
Ответ: неоправданных ограничений при работе в сети (системе)

Оценочные средства для формирования компетенции ОПК – 4 в процессе освоения дисциплины (модуля)

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

Индикаторы достижения компетенции

Выполняет участие в разработке технологической и эксплуатационной документации.

1. Принципом политики информационной безопасности является принцип:
1) Невозможности миновать защитные средства сети (системы)
2) Усиления основного звена сети, системы
3) Полного блокирования доступа при риск-ситуациях

2. Принципом политики информационной безопасности является принцип:
1) Усиления защищенности самого незащищенного звена сети (системы)
2) Перехода в безопасное состояние работы сети, системы
3) Полного доступа пользователей ко всем ресурсам сети, системы

3. Принципом политики информационной безопасности является принцип:
1) Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
2) Одноуровневой защиты сети, системы
3) Совместимых, однотипных программно-технических средств сети, системы

4. К основным типам средств воздействия на компьютерную сеть относится:
1) Компьютерный сбой
2) Логические закладки («мины»)
3) Аварийное отключение питания

5. Когда получен спам по e-mail с приложенным файлом, следует:
1) Прочитать приложение, если оно не содержит ничего ценного – удалить
2) Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
3) Удалить письмо с приложением, не раскрывая (не читая) его

6. Принцип Кирхгофа:
Ответ: секретность закрытого сообщения определяется секретностью ключа

7. ЭЦП – это:
Ответ: электронно-цифровая подпись

8. Наиболее распространены угрозы информационной безопасности корпоративной системы:
Ответ: ошибки эксплуатации и неумышленного изменения режима работы системы

9. Наиболее распространены угрозы информационной безопасности сети:
Ответ: сбой (отказ) оборудования, нелегальное копирование данных

10) Наиболее распространены средства воздействия на сеть офиса:
Ответ: вирусы в сети, логические мины (закладки), информационный перехват