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

УТВЕРЖДАЮ
Директор филиала КузГТУ
_____ Т.А. Евсина
«29» мая 2023 г.

Фонд оценочных средств дисциплины
Основы информационной безопасности

Специальность
«10.02.05 Обеспечение информационной безопасности автоматизированных систем»

Присваиваемая квалификация
«Техник по защите информации»

Форма обучения
очная

Год набора 2023

Срок обучения на базе
среднего общего образования – 2 года 10 месяцев

Новокузнецк 2023 г.

1. Фонд оценочных средств для проведения текущего контроля, промежуточной аттестации обучающихся по дисциплине

1.1 Паспорт фонда оценочных средств

Планируемые результаты обучения по дисциплине.

Дисциплина направлена на формирование следующих компетенций выпускника:

№ п/п	Наименование разделов	Содержание (темы) раздела	Код компетенции	Знания, умения, практический опыт, необходимые для формирования соответствующей компетенции	Форма текущего контроля знаний, умений, практического опыта, необходимых для формирования соответствующей компетенции
1	Раздел 1. Теоретические основы информационной безопасности	Тема 1.1. Основные понятия и задачи информационной безопасности Тема 1.2. Основы защиты информации Тема 1.3. Угрозы безопасности защищаемой информации.	ОК 03	**Знать:** современные средства и способы обеспечения информационной безопасности; основные методики анализа угроз и рисков информационной безопасности. **Уметь:** классифицировать основные угрозы безопасности информации	опрос обучающихся по контрольным вопросам, защита отчетов по практическим заданиям, тестирование
			ОК 06	**Знать:** место информационной безопасности в системе национальной безопасности страны. **Уметь:** классифицировать основные угрозы безопасности информации	
			ОК 09	**Знать:** сущность и понятие информационной безопасности, характеристику ее составляющих. **Уметь:** классифицировать основные угрозы безопасности информации	
			ОК 10	**Знать:** источники угроз безопасности информации и меры по их предотвращению. **Уметь:** классифицировать основные угрозы безопасности информации.	
			ПК 2.4	**Знать:** виды, источники и носители защищаемой информации; факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах; жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи. **Уметь:** классифицировать защищаемую информацию по видам тайны и степеням секретности **Иметь практический опыт:**	

				- обработки, хранения и передачи информации	
2	Раздел 2. Методология защиты информации	Тема 2.1. Методологические подходы к защите информации Тема 2.2. Нормативно правовое регулирование защиты информации Тема 2.3. Защита информации в автоматизированных (информационных) системах	ОК 03	**Знать:** современные средства и способы обеспечения информационной безопасности; основные методики анализа угроз и рисков информационной безопасности. **Уметь:** классифицировать основные угрозы безопасности информации	опрос обучающихся по контрольным вопросам, защита отчетов по практическим заданиям, тестирование
			ОК 06	**Знать:** место информационной безопасности в системе национальной безопасности страны. **Уметь:** классифицировать основные угрозы безопасности информации	
			ОК 09	**Знать:** сущность и понятие информационной безопасности, характеристику ее составляющих. **Уметь:** классифицировать основные угрозы безопасности информации	
			ОК 10	**Знать:** источники угроз безопасности информации и меры по их предотвращению. **Уметь:** классифицировать основные угрозы безопасности информации.	
			ПК 2.4	**Знать:** виды, источники и носители защищаемой информации; факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах; жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи. **Уметь:** классифицировать защищаемую информацию по видам тайны и степеням секретности **Иметь практический опыт:** - обработки, хранения и передачи информации	

1.2 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 КузГТУ, в том числе синхронного и (или) асинхронного взаимодействия посредством сети «Интернет».

1.2.1 Оценочные средства при текущем контроле

Текущий контроль по темам дисциплины заключается в опросе обучающихся по контрольным вопросам и (или) тестировании, и (или) практических работ (при наличии).

При проведении текущего контроля обучающимся письменно, либо устно необходимо ответить на 2 вопроса, выбранных случайным.

ПРИМЕРНЫЕ ВОПРОСЫ:

Критерии оценивания при текущем контроле:

- 85–100 баллов – при правильном и полном ответе на два вопроса;
- 65–84 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 25–64 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-24	25-64	65-84	85-100
Школа оценивания	2	3	4	5

Например вопросы:

Вопрос	Ответ
Сведения (сообщения, данные) независимо от формы их представления – это	Информация
Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов – это	Информационные технологии
Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации – это	Обладатель информации
Технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники – это	Информационно-телекоммуникационная сеть

ПРИМЕРНОЕ ТЕСТИРОВАНИЕ

Тестирование включает как тесты с выбором ответа, так и задачи с вычисляемым ответом. Последний тип заданий формируется таким образом, чтобы верное решение задания демонстрировало владение материалом курса, но не требовало сложных вычислений. За час обучающийся должен ответить на 10 вопросов теста. Тест формируется таким образом, чтобы охватывать все темы, изучаемые в семестре, а вопрос по каждой теме попадает в тест случайным образом. Каждый верный ответ оценивается в 10 баллов.

Критерии оценивания:

90-100 баллов – при правильном ответе на 90-100%.
80-89 баллов – при правильном ответе на 80-89 %.
60-79 балла – при правильном ответе на 60-79 %.
0-59 баллов – при правильном ответе на менее 59 %.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	2	3	4	5

Пример тестирования:

Вопрос	Ответ
Сведения (сообщения, данные) независимо от формы их представления: А) информация Б) информационные технологии В) информационная система Г) информационно-телекоммуникационная сеть Д) обладатель информации	А
Информация, зафиксированная на материальном носителе, с реквизитами, позволяющими ее идентифицировать, называется А) Достоверной Б) Конфиденциальной В) Документированной Г) коммерческой тайной	В

Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации: А) источник информации Б) потребитель информации В) уничтожитель информации Г) носитель информации Д) обладатель информации	Д
Отношения, связанные с обработкой персональных данных, регулируются_____ А) «об информации, информационных технологиях» Б) «о защите информации» В) федеральным законом «о персональных данных» Г) федеральным законом «о конфиденциальной информации» Д) «об утверждении перечня сведений конфиденциального характера»	В

1.2.2 Оценочные средства при промежуточной аттестации

Формой промежуточной аттестации является **дифференцированный зачёт (зачёт с оценкой) в 1 семестре,** в процессе которого определяется сформированность обозначенных в рабочей программе компетенций.

Зачет с оценкой проводится либо в форме опроса по контрольным вопросам, либо в форме компьютерного тестирования.

Опрос по контрольным вопросам

Во время опроса по контрольным вопросам обучающимся задается два вопроса выбранных случайным образом.

Критерии оценивания

- 85–100 баллов – при правильном и полном ответе на два вопроса;
- 65–84 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 25–64 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-24	25-64	65-84	85-100
Школа оценивания	2	3	4	5

Например вопросы:

Вопрос	Ответ
Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя – это	Конфиденциальность информации
Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц – это	распространение информации
Возможность получения информации и ее использования – это	доступ к информации
Информация, переданная или полученная пользователем информационно-телекоммуникационной сети – это	электронное сообщение

ПРИМЕРНОЕ ТЕСТИРОВАНИЕ

Тестирование включает как тесты с выбором ответа, так и задачи с вычисляемым ответом. Последний тип заданий формируется таким образом, чтобы верное решение задания демонстрировало владение материалом курса, но не требовало сложных вычислений. За час обучающийся должен ответить на 10 вопросов теста. Тест формируется таким образом, чтобы охватывать все темы, изучаемые в семестре, а вопрос по каждой теме попадает в тест случайным образом. Каждый верный ответ оценивается в 10 баллов.

Критерии оценивания:

90-100 баллов – при правильном ответе на 90-100%.
80-89 баллов – при правильном ответе на 80-89 %.
60-79 балла – при правильном ответе на 60-79 %.
0-59 баллов – при правильном ответе на менее 59 %.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	2	3	4	5

Вопрос	Ответ
К конфиденциальной информации относятся документы, содержащие _____ А) государственную тайну Б) законодательные акты	А

В) ноу-хау сведения о золотом запасе страны	
Система защиты государственных секретов определяется Законом А) "Об информации, информатизации и защите информации" Б) "Об органах ФСБ" В) "О государственной тайне" Г) "О безопасности.	В
Действие Закона "О государственной тайне" распространяется А) на всех граждан и должностных лиц РФ Б) только на должностных лиц В) на граждан, которые взяли на себя обязательство выполнять требования Г) законодательства о государственной тайне на всех граждан и должностных лиц, если им предоставили для работы закрытые сведения	Д
По принадлежности информационные ресурсы подразделяются на А) государственные, коммерческие и личные Б) государственные, не государственные и информацию о гражданах В) информацию юридических и физических лиц официальные, гражданские и коммерческие	А

Оценочные средства для формирования компетенции

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

Задания закрытого типа

Вопрос	Ответ
Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется: А) активный перехват; Б) пассивный перехват; В) аудиоперехват; Г) видеоперехват; Д) просмотр мусора.	Б
Перехват, который осуществляется путем использования оптической техники называется: А) активный перехват; Б) пассивный перехват; В) аудиоперехват; Г) видеоперехват; Д) просмотр мусора	Г
Для безопасной передачи данных по каналам интернет используется технология: 1. WWW 2. DICOM 3. VPN 4. FTP 5. XML	3
Комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию сетевого трафика в соответствии с заданными правилами и защищающий компьютерные сети от несанкционированного доступа: 1. Антивирус 2. Замок 3. Брандма́уэр 4. Криптография 5. Экспертная система	3
За правонарушения в сфере информации, информационных технологий и защиты информации данный вид наказания на сегодняшний день <u>не предусмотрен</u>: 1. Дисциплинарные взыскания 2. Административный штраф 3. Уголовная ответственность	5

4. Лишение свободы 5. Смертная казнь	

Задания открытого типа

Вопрос	Ответ
Все компоненты информационной системы предприятия, в котором накапливаются и обрабатываются персональные данные – это	информационная система персональных данных
Действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных – это	деперсонификация
В статье 272 уголовного кодекса говорится…	О неправомерном доступе к компьютерной информации
Федеральный закон «об информации, информатизации и защите информации» направлен на:	Регулирование взаимоотношений в информационной сфере совместно с гражданским кодексом РФ
Хищение информации – это…	Несанкционированное копирование информации

Оценочные средства для формирования компетенции
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
Задания закрытого типа

Вопрос	Ответ
Несанкционированный доступ к информации это: 1. Доступ к информации, не связанный с выполнением функциональных обязанностей и не оформленный документально 2. Работа на чужом компьютере без разрешения его владельца 3. Вход на компьютер с использованием данных другого пользователя 4. Доступ к локально-информационной сети, связанный с выполнением функциональных обязанностей 5. Доступ к субд под запрещенным именем пользователя	1
Персональные данные» это: 1. Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу 2. Фамилия, имя, отчество физического лица 3. Год, месяц, дата и место рождения, адрес физического лица 4. Адрес проживания физического лица 5. Сведения о семейном, социальном, имущественном положении человека, составляющие понятие «профессиональная тайна»	1
В данном случае сотрудник учреждения может быть привлечен к ответственности за нарушения правил информационной безопасности: 1. Выход в интернет без разрешения администратора 2. При установке компьютерных игр 3. В случаях установки нелицензионного ПО 4. В случае не выхода из информационной системы 5. В любом случае неправомочного использования конфиденциальной информации при условии письменного предупреждения сотрудника об ответственности	5
Может ли сотрудник быть привлечен к уголовной ответственности за нарушения правил информационной безопасности предприятия: 1. Нет, только к административной ответственности 2. Нет, если это государственное предприятие 3. Да 4. Да, но только в случае, если действия сотрудника нанесли непоправимый вред 5. Да, но только в случае осознанных неправомочных действий сотрудника	3

Процедура, проверяющая, имеет ли пользователь с предъявленным идентификатором право на доступ к ресурсу это: 1. Идентификация 2. Аутентификация 3. Стратификация 4. Регистрация 5. Авторизация	2

Задания открытого типа

Вопрос	Ответ
Владельцем информации первой категории является…	Муниципальное учреждение
Владельцем информации второй категории является…	Простые люди
Владельцем информации третьей категории является…	Государство
Информацией, составляющей государственную тайну, владеют:	Государство
Информацией, составляющей коммерческую тайну, владеют:	Различные учреждения

Оценочные средства для формирования компетенции
ОК 09. Использовать информационные технологии в профессиональной деятельности.
Задания закрытого типа

Вопрос	Ответ
Наиболее опасным источником угроз информационной безопасности предприятия являются: 1. Другие предприятия (конкуренты) 2. Сотрудники информационной службы предприятия, имеющие полный доступ к его информационным ресурсам 3. Рядовые сотрудники предприятия 4. Возможные отказы оборудования, отключения электропитания, нарушения в сети передачи данных 5. Хакеры	3
Выберите, можно ли в служебных целях использовать электронный адрес (почтовый ящик), зарегистрированный на общедоступном почтовом сервере, например на mail.ru: 1. Нет, не при каких обстоятельствах 2. Нет, но для отправки срочных и особо важных писем можно 3. Можно, если по нему пользователь будет пересылать информацию, не содержащую сведений конфиденциального характера 4. Можно, если информацию предварительно заархивировать с помощью программы WINRAR с паролем 5. Можно, если других способов электронной передачи данных на предприятии или у пользователя в настоящий момент нет, а информацию нужно переслать срочно	1
НАИБОЛЕЕ ОПАСНЫМ ИСТОЧНИКОМ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ ЯВЛЯЮТСЯ: 1. Другие предприятия (конкуренты) 2. Сотрудники информационной службы предприятия, имеющие полный доступ к его информационным ресурсам 3. Рядовые сотрудники предприятия 4. Возможные отказы оборудования, отключения электропитания, нарушения в сети передачи данных 5. Хакеры	3
Выберите, можно ли в служебных целях использовать электронный адрес (почтовый ящик), зарегистрированный на общедоступном почтовом сервере, например на mail.ru: 1. Нет, не при каких обстоятельствах 2. Нет, но для отправки срочных и особо важных писем можно 3. Можно, если по нему пользователь будет пересылать информацию, не содержащую сведений конфиденциального характера 4. Можно, если информацию предварительно заархивировать с помощью программы winrar с паролем	1

5. Можно, если других способов электронной передачи данных на предприятии или у пользователя в настоящий момент нет, а информацию нужно переслать срочно	
Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности? Варианты ответа: а) Сотрудники б) Хакеры в) Атакующие г) Контрагенты (лица, работающие по договору)	А

Задания открытого типа

Вопрос	Ответ
Одно или несколько слов, являющиеся любыми частями речи, которые в наибольшей степени отражает содержание всего искомого документа - это	Ключевое слово
Что обеспечивает информационная безопасность?	Сохранность информации
Доступ к информации - это:	Возможность получения информации и ее использования
Вопросы информационного обмена регулируются (...) правом	Гражданским
Наименьшая единица, необходимая для организации поиска информации в справочно - правовых системах - это	Слово

Оценочные средства для формирования компетенции
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.
Задания закрытого типа

Вопрос	Ответ
Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству? **Варианты ответа:** а) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования б) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации в) Улучшить контроль за безопасностью этой информации г) Снизить уровень классификации этой информации	В
Что самое главное должно продумать руководство при классификации данных? Варианты ответа: а) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным б) Необходимый уровень доступности, целостности и конфиденциальности в) Оценить уровень риска и отменить контрмеры г) Управление доступом, которое должно защищать данные	Б
Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены? Варианты ответа: а) Владельцы данных б) Пользователи в) Администраторы г) Руководство	Г
Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют: Варианты ответа: а) Внедрение управления механизмами безопасности б) Классификацию данных после внедрения механизмов безопасности в) Уровень доверия, обеспечиваемый механизмом безопасности г) Соотношение затрат / выгод	В

Защита информации: а) небольшая программа для выполнения определенной задачи б) комплекс мероприятий, направленных на обеспечение информационной безопасности в) процесс разработки структуры базы данных в соответствии с требованиями пользователей	Б

Задания открытого типа

Вопрос	Ответ
На что классифицируют по доступности информацию	информацию с ограниченным доступом и общедоступную информацию
Наиболее опасным источником угроз информационной безопасности предприятия являются	Рядовые сотрудники предприятия
Нежелательная цепочка носителей информации, один или несколько из которых являются правонарушителем или его специальной аппаратурой называется	Канал утечки информации
Доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации называется	Несанкционированный доступ к информации
Продолжите фразу: "Административная и законодательная мера, соответствующая мере ответственности лица за потерю конкретной секретной информации, регламентирующаяся специальным документом с учетом государственных и военно-стратегических, коммерческих или частных интересов - это..."	Уровень секретности

Оценочные средства для формирования компетенции

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

Задания закрытого типа

Вопрос	Ответ
Процедурой называется: а) пошаговая инструкция по выполнению задачи б) обязательные действия в) руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах	А
Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании: а) проведение тренингов по безопасности для всех сотрудников б) поддержка высшего руководства в) эффективные защитные меры и методы их внедрения	Б
Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков: а) когда риски не могут быть приняты во внимание по политическим соображениям б) для обеспечения хорошей безопасности нужно учитывать и снижать все риски в) когда стоимость контрмер превышает ценность актива и потенциальные потери	В
Что такое политика безопасности: а) детализированные документы по обработке инцидентов безопасности б) широкие, высокоуровневые заявления руководства в) общие руководящие требования по достижению определенного уровня безопасности	Б
Какая из приведенных техник является самой важной при выборе конкретных защитных мер: а) анализ рисков б) результаты ALE в) анализ затрат / выгоды	В

Задания открытого типа

Вопрос	Ответ

Какие программы относят к разряду вредоносных?	К вредоносному программному обеспечению относятся сетевые черви, классические файловые вирусы, троянские программы, хакерские утилиты и прочие программы, наносящие вред компьютеру
Что такое ПЭМИН?	ПЭМИН – побочные электромагнитные излучения и наводки данных излучений на токоведущие конструкции, линии и подключенные к ним технические средства
Вирус, поражающий документы называется	Макровирус
Абстрактное содержание какого-либо высказывания, описание, указание, сообщение либо известие - это	Информация
Информация может быть защищена без аппаратных и программных средств защиты с помощью _____ преобразований.	Криптографических

1.2.3 Методические материалы, определяющие процедуры оценивания знаний, умений, практического опыта деятельности, характеризующие этапы формирования компетенций

Порядок организации проведения текущего контроля и промежуточной аттестации представлен в Положении о проведении текущего контроля и промежуточной аттестации обучающихся, осваивающих образовательные программы среднего профессионального образования в КузГТУ (Ип 06/10)