Федеральное агентство по рыболовству
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Калининградский государственный технический университет»
(ФГБОУ ВО «КГТУ»)

УТВЕРЖДАЮ
Начальник УРОПСП

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
ФГБОУ ВО «КГТУ»
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат:
0174a99400e2af6fb74dca3b394e65efc4
Владелец: Мельникова Виктория Александровна
Действителен: с 12.04.2023 по 12.04.2024

Фонд оценочных средств
(приложение к рабочей программе дисциплины)

«ВВЕДЕНИЕ В СПЕЦИАЛЬНОСТЬ»

основной профессиональной образовательной программы специалитета
по специальности

10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специализация

«БЕЗОПАСНОСТЬ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ»

ИНСТИТУТ	Институт цифровых технологий
РАЗРАБОТЧИК	Кафедра информационной безопасности

1 РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Таблица 1 – Планируемые результаты обучения по дисциплине, соотнесенные с установленными индикаторами достижения компетенций

Код и наименование компетенции	Индикаторы достижения компетенции	Дисциплина	Результаты обучения (владения, умения и знания), соотнесенные с компетенциями/индикаторами достижения компетенции
УК-6: Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни; ПК-3: Способен выявлять основные угрозы безопасности информации в автоматизированных системах	УК-6.2: Планирует траекторию своего профессионального развития и предпринимает шаги по её реализации; ПК-3.1: Использует знания о структуре системы защиты от угроз нарушения конфиденциальности, целостности, доступности, эталонную модель взаимодействия открытых информационных систем	Введение в специальность	*Знать:* - основные информационные технологии, используемые в автоматизированных системах; - системы управления информационной безопасностью открытой информационной системы; - основную терминологию в области информационной безопасности; современные тренды развития в профессиональной сфере; - историю развития теории компьютерной безопасности. *Уметь:* - анализировать представленную в общедоступных источниках информацию о современных тенденциях в области информационных систем. *Владеть:* - основными сведениями из учебного плана изучаемых дисциплин для планирования своей личной траектории профессионального развития.

2 ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ И КРИТЕРИИ ОЦЕНИВАНИЯ

2.1 Для оценки результатов освоения дисциплины используются:

- оценочные средства текущего контроля успеваемости;

- оценочные средства для промежуточной аттестации по дисциплине.

2.2 К оценочным средствам для текущего контроля успеваемости относятся:

- тестовые задания.

2.3 К оценочным средствам для промежуточной аттестации по дисциплине, проводимой в форме зачета, относятся:

Промежуточная аттестация в форме зачета проходит по результатам прохождения всех видов текущего контроля успеваемости в течение семестра.

3 ОЦЕНОЧНЫЕ СРЕДСТВА ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

3.1. Типовые тестовые вопросы для текущей аттестации приведены в Приложении 1.

При оценке результатов за каждый правильный ответ ставится 1 балл, за неправильный ответ – 0 баллов.

Тестовые оценки соотносятся с пятибалльной системой:

- оценка «5» (отлично) выставляется студентам за верные ответы, которые составляют 90 % и более от общего количества вопросов;

- оценка «4» (хорошо) соответствует результатам тестирования, которые содержат от 70 % до 80 % правильных ответов;

- оценка «3» (удовлетворительно) от 50 % до 60 % правильных ответов;

- оценка «2» (неудовлетворительно) соответствует результатам тестирования, содержащие менее 50 % правильных ответов

4 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

Промежуточная аттестация в форме зачета проходит по результатам прохождения всех видов текущего контроля успеваемости в течение семестра.

5. СВЕДЕНИЯ О ФОНДЕ ОЦЕНОЧНЫХ СРЕДСТВ И ЕГО СОГЛАСОВАНИИ

Фонд оценочных средств для аттестации по дисциплине «Введение в специальность» представляет собой компонент основной профессиональной образовательной программы специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация «Безопасность открытых информационных систем»).

Фонд оценочных средств рассмотрен и одобрен на заседании кафедры информационной безопасности 20.04.2022 г. (протокол № 7).

Заведующая кафедрой  Н.Я. Великите

Приложение 1

ТЕСТОВЫЕ ВОПРОСЫ И ЗАДАНИЯ ПО ДИСЦИПЛИНЕ

Вариант 1

1. _____ – предоставление определенных полномочий лицу (группе лиц) на выполнение некоторых действий в системе обработки данных.
2. _____ - свойство информации, заключающееся в ее существовании в неизменном виде (по отношению к некоторому фиксированному ее состоянию) в условиях случайного и (или) преднамеренного искажения (разрушения).
3. _____- это совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации
4. _____ – субъект, действия которого нарушают безопасность информации в рассматриваемой компьютерной системе.
5. _____ - это присвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку присвоенных.
6. _____ - программы, предотвращающие заражение компьютерным вирусом и ликвидирующие последствия заражения.
7. _____- программа, выполняемая периодически или в определенный момент времени с целью исказить, уничтожить или модифицировать данные.
8. _____ - антивирусная программа, распознающая известные ей вирусы по характерным участкам их кода.
9. _____ – криптографическое преобразование данных для получения шифрованного текста.
10. _____– это любая программа, разработанная с целью выявления или использования уязвимостей в другом ПО.
11. Электронный ресурс, на котором находится актуальна методика моделирования угроз безопасности информации:

1. ФСТЭК России
2. ФСБ России
3. Министерство цифрового развития России
4. Минэкономразвития России

12. _____ – это сочетание инструментов, используемых для выявления, защиты и устранения событий безопасности, угрожающих вашей ИТ-системе, с использованием данных в реальном времени и исторических данных.

13. _____– это специалист, основной задачей которого является обеспечение штатной работы компьютерной техники, сети и программного обеспечения в организации.

Вариант 2

1. _____– проверка принадлежности субъекта доступа предъявленного им идентификатора, подтверждение подлинности.
2. _____- субъективно определяемая (приписываемая) информации характеристика (свойство), указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней.
3. _____ - подверженность информации воздействию различных дестабилизирующих факторов, которые могут привести к нарушению ее конфиденциальности, целостности, доступности, или неправомерному ее тиражированию.
4. _____ - доступ, содержащий различные виды нарушения правил по пользованию данными.
5. _____ - некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации.
6. _____ – сочетание программного и аппаратного обеспечения, образующее систему защиты от несанкционированного доступа к компьютеру из внешней глобальной или локальной сети.
7. _____ – наука, изучающая способы тайной передачи сообщений.
8. _____ – уникальная характеристика системы, которая может быть проверена. Примером С. может служить признак диска, используемый в качестве идентификационной метки диска-оригинала; этот признак не должен копироваться программным способом.
9. _____ – пользователь, который пытается вносить изменения в системное ПО, не имея на это право.
10. _____- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

11. Расшифровка аббревиатуры ФСТЭК:

1. Федеральная служба технической эксплуатации.
2. Федеральная служба технического и экспортного контроля.
3. Федеральная сеть технических и экономических комиссий

12. Аналитика безопасности важна, поскольку позволяет _____до того, как они повлияют на вашу систему.

13. _____в классическом понимании — это создание законченной взаимоувязанной подсистемы ИБ в соответствии с потребностями заказчика, состоянием информационной системы (ИС), а также перспективами роста и развития ИС. Как правило, реализация полного интеграционного проекта включает три стадии: консалтинг (анализ рисков, построение модели угроз, проектирование системы), поставки программно-аппаратных средств защиты информации и их внедрение.

Вариант 3

1. Под _____ понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.
2. _____ - свойство системы, в которой циркулирует информация (средств и технологии ее обработки), характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.
3. _____– это формальное изложение правил поведения, процедур, практических приемов или руководящих принципов в области информационной безопасности, которыми руководствуется организация в своей деятельности
4. _____не контролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации иностранными разведками
5. _____ - некоторое уникальное количество информации, позволяющее различать индивидуальных пользователей парольной системы (проводить их идентификацию).
6. _____ – программа, способная самопроизвольно создавать свои копии и модифицирующая другие программы, записанные в файлах или системных областях, для последующего получения управления и воспроизводства новой копии.

7. _____ – утеря критичности информации или получение ее неавторизованными для этого субъектами (лицами, программами, процессами и т. д.).

8. _____ - вирус, который оставляет в памяти компьютера модули, перехватывающие обращение программ к дискам.

9. _____ – часть формата элемента данных из одного или нескольких битов, которые определяют его статус.

10. _____ – компьютерный эквивалент обычной подписи под документом, который должен обеспечить подлинность документа и защитить передаваемое сообщение от изменений.

11. Этот федеральный орган исполнительной власти, в пределах своих полномочий осуществляющий государственное управление в области обеспечения безопасности Российской Федерации, защиты и охраны государственной границы Российской Федерации, охраны внутренних морских вод, территориального моря, исключительной экономической зоны, континентального шельфа Российской Федерации и их природных ресурсов, обеспечивающий информационную безопасность Российской Федерации и непосредственно реализующий основные направления деятельности органов федеральной службы безопасности, определенные законодательством Российской Федерации, а также координирующий контрразведывательную деятельность федеральных органов исполнительной власти, имеющих право на ее осуществление.

1. ФСБ России

2.ФСТЭК России

3.Минкомсвязи России

4.Роскомнадзор

12. Специалист в сфере информационной безопасности, осуществляющий тест на проникновение - _____.

13. _____— это поставщик, который продает и продвигает товары и услуги под собственным брендом или торговой маркой. При этом он не всегда самостоятельно производит товар, его ключевая задача — продвижение и реализация.