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

УТВЕРЖДАЮ
И.о. директора института

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
ФГБОУ ВО «КГТУ»
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат: 4ae0684d0d529bb9d0248a5b51302ea1
Владелец: Гоконаев Мирослав Валерьевич
Действителен: с 02.08.2024 по 26.10.2025

Фонд оценочных средств
(приложение к рабочей программе модуля)

«АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

основной профессиональной образовательной программы специалитета
по специальности

10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специализация

"БЕЗОПАСНОСТЬ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ"

ИНСТИТУТ	цифровых технологии
РАЗРАБОТЧИК	кафедра информационной безопасности

1 РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ, ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ И КРИТЕРИИ ОЦЕНИВАНИЯ

1.1 Результаты освоения дисциплины

Таблица 1 – Планируемые результаты обучения по дисциплине, соотнесенные с установленными компетенциями

Код и наименование компетенции	Дисциплина	Результаты обучения (владения, умения и знания), соотнесенные с компетенциями
ОПК-15: Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	Аудит информационной безопасности	Знания: 1. Способы защиты информации от несанкционированного доступа и утечки по техническим каналам 2. Принципы построения систем защиты информации 3. Нормативные правовые акты в области защиты информации 4. Организационные меры по защите информации 5. Способы инструментального мониторинга автоматизированных систем Умения: 1. Классифицировать и оценивать угрозы безопасности информации для объекта информатизации 2. Разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем 3. Применять инструментальные средства контроля защищенности

		информации в автоматизированных системах Навыки: 1. Оценка информационных рисков безопасности информации в автоматизированной системе 2. Обоснование и контроль результатов управленческих решений в области безопасности информации автоматизированных систем 3. Экспертиза состояния защищенности информации автоматизированных систем 4. Обоснование критериев эффективности функционирования защищенных автоматизированных систем

1.2 К оценочным средствам текущего контроля успеваемости относятся:

- тестовые задания открытого и закрытого типов.

К оценочным средствам для промежуточной аттестации относятся:

- экзаменационные задания по дисциплине, представленные в виде тестовых заданий закрытого и открытого типов.

1.3 Критерии оценки результатов освоения дисциплины

Универсальная система оценивания результатов обучения включает в себя системы оценок: 1) «отлично», «хорошо», «удовлетворительно», «неудовлетворительно»; 2) «зачтено», «не зачтено»; 3) 100 – балльную/процентную систему и правило перевода оценок в пятибалльную систему (табл. 2).

Таблица 2 – Система оценок и критерии выставления оценки

Система оценок / Критерий	2	3	4	5
	0-40%	**41-60%**	**61-80 %**	**81-100 %**
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	«не зачтено»	**«зачтено»**		
1 Системность и полнота знаний в отношении изучаемых объектов	Обладает частичными и разрозненными знаниями, которые не может научно- корректно связывать между собой (только некоторые из которых может связывать между собой)	Обладает минимальным набором знаний, необходимым для системного взгляда на изучаемый объект	Обладает набором знаний, достаточным для системного взгляда на изучаемый объект	Обладает полнотой знаний и системным взглядом на изучаемый объект
2 Работа с информацией	Не в состоянии находить необходимую информацию, либо в состоянии находить отдельные фрагменты информации в рамках поставленной задачи	Может найти необходимую информацию в рамках поставленной задачи	Может найти, интерпретировать и систематизировать необходимую информацию в рамках поставленной задачи	Может найти, систематизировать необходимую информацию, а также выявить новые, дополнительные источники информации в рамках поставленной задачи
3 Научное осмысление изучаемого явления, процесса, объекта	Не может делать научно корректных выводов из имеющихся у него сведений, в состоянии проанализировать только некоторые из имеющихся у него сведений	В состоянии осуществлять научно корректный анализ предоставленной информации	В состоянии осуществлять систематический и научно корректный анализ предоставленной информации, вовлекает в исследование новые релевантные задаче данные	В состоянии осуществлять систематический и научно-корректный анализ предоставленной информации, вовлекает в исследование новые релевантные поставленной задаче данные, предлагает новые ракурсы поставленной задачи
4 Освоение стандартных алгоритмов решения профессиональных задач	В состоянии решать только фрагменты поставленной задачи в соответствии с заданным алгоритмом, не освоил предложенный алгоритм, допускает ошибки	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом, понимает основы предложенного алгоритма	Не только владеет алгоритмом и понимает его основы, но и предлагает новые решения в рамках поставленной задачи

1.4 Оценивание тестовых заданий закрытого типа осуществляется по системе зачтено/ не зачтено («зачтено» – 41-100% правильных ответов; «не зачтено» – менее 40 % правильных ответов) или пятибалльной системе (оценка «неудовлетворительно» - менее 40 % правильных ответов; оценка «удовлетворительно» - от 41 до 60 % правильных ответов; оценка «хорошо» - от 61 до 80% правильных ответов; оценка «отлично» - от 81 до 100 % правильных ответов).

Тестовые задания открытого типа оцениваются по системе «зачтено/ не зачтено». Оценивается верность ответа по существу вопроса, при этом не учитывается порядок слов в словосочетании, верность окончаний, падежи.

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Компетенция ОПК-15: Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем.

Тестовые задания открытого типа:

1. Термин означающий, что данные не были изменены при выполнении какой-либо операции над ними, будь то передача, хранение или отображение это:_____

Ответ: целостность

2. Вероятность возникновения негативного события, которое нанесет ущерб организации или физическому лицу это: _____

Ответ: риск информационной безопасности

3. По типу источника возникновения угрозы информационной безопасности бывают:

Ответ: техногенные, антропогенные, стихийные явления

4. Федеральный орган исполнительной власти России, осуществляющий реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности – это_____

Ответ: ФСТЭК России

5. Определите класс автоматизированной системы по следующим классификационным признакам: *многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. И все пользователи имеют*

равные права доступа ко всей информации АС, обрабатывается "Служебная тайна" и общедоступная информация:" _____

Ответ: 2Б

6. Методы и средства защиты информации бывают:_____

Ответ: технические (программные) и аппаратные

7. Слабость в средствах защиты и некое неблагоприятное свойство информационной системы, которую можно использовать
для нарушения свойств безопасности системы или содержащейся в ней информации это:

Ответ: уязвимость

8. Собрание участников безопасности, имеющих единый центр, использующий единую базу, единую групповую и локальную политики, ограничение времени работы учётной записи и прочие параметры, значительно упрощающие работу системного администратора организации, если в ней эксплуатируется большое число компьютеров это:

Ответ: домен безопасности

9. Укажите порядок задания прав доступа в ОС Linux:

Ответ: владелец-группа-остальные

10. Окончательно, ответственность за защищенность данных в компьютерной сети несет:

Ответ: владелец сети

11. Процесс получения объективных качественных и количественных оценок о текущем состоянии защищенности информационных ресурсов компании в соответствии с российскими и международными нормативами это:

Ответ: комплексный аудит информационной безопасности

12. Исследование состояния защищенности информационной системы с точки зрения хакера (или некоего злоумышленника, обладающего высокой квалификацией в области информационных технологий) это:

Ответ: активный аудит

13. Совокупность условий и факторов, создающих опасность нарушения информационной безопасности, потенциально возможное событие, действие (воздействие), процесс или явление, которые могут привести к нанесению ущерба чьим-либо интересам это:

Ответ: угроза

14. Минимальная длина пароля в случае смены ежеквартально должна быть:

Ответ: 12 символов

15. Категория мошенников является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности это:

Ответ: сотрудники

16. Пошаговая инструкция по выполнению задачи – это:

Ответ: процедура

17. Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

Ответ: защищаемой

18. Вид анализа позволяет оценить факт выполнения условий функционирования системы с заданной степенью вероятности называется:

Ответ: статистический

19. Главная цель создания информационных систем это:

Ответ: получение информационных услуг

20. Наиболее распространены угрозы информационной безопасности сети:

Ответ: нелегальное копирование данных

21. Наиболее распространены средства воздействия на сеть офиса:

Ответ: вирусы

22. Вид анализа, который позволяет оценить факт выполнения условий функционирования системы в заданном варианте структуры при номинальных значениях внутренних параметров называется:

Ответ: одновариантный

Тестовые задания закрытого типа:

23. Требование, являющиеся необязательным для операционных систем, сертифицированных по 5 классу РД СВТ:

1. Должны быть предусмотрены средства управления, ограничивающие распространение прав на доступ

3. Контроль доступа должен быть применим к каждому объекту и каждому субъекту (индивиду или группе равноправных индивидов)

2. ОС должна содержать механизм, претворяющий в жизнь дискреционные правила разграничения доступа

4. **В ОС должен быть реализован диспетчер доступа, т.е. средство, осуществляющее перехват всех обращений субъектов к объектам, а также разграничение доступа в соответствии с заданным принципом разграничения доступа**

24. Функцией центров защиты информации **НЕ** является:

1. участие в исследованиях и разработках основных вопросов защиты информации

3. гарантированное уничтожение сведений о средствах защиты

2. аккумулирование всех новейших достижений в области защиты информации

4. оказание конкретным объектам — абонентам услуг по созданию, организации и обеспечению функционирования систем защиты

25: РАМ это набор открытых библиотек подключаемых модулей_____

1. аутентификации

3. доверенной загрузки

2. резервного восстановления

4. шифрования

26. Контроль организации и обеспечения работы с конфиденциальной информацией **НЕ** предполагает:

1. наличие в каждом структурном подразделении функциональных обязанностей (задачи, функции, права с учетом обязанностей)

3. изменение размеров контролируемой зоны

2. распределение прав доступа к конфиденциальной информации по степени важности и по отраслям

4. учет криптографических средств защиты информации, соответствие установленного порядка обращения с ключами

27. Классами защищённости автоматизированных систем от несанкционированного доступа являются:

1. 1Е

3. 2Б

2. 2А

4. 3В

28. В задачи поисковых мероприятий **НЕ** входит:

1. определение состояния информационной безопасности объекта
3. выдача рекомендаций по оптимальным способам блокирования каналов утечки информации
2. поиск установленных приборов и систем перехвата и передачи информации
4. блокирование каналов утечки информации

29. Методологическая база управления проектами **НЕ** предполагает:

1. обследование объектов и среды для предварительной формализации целей, назначения и задач проекта
3. сравнение альтернатив по величине достигаемого эффекта в зависимости от затрат на его достижение (показатель эффективность/стоимость)
2. исключение альтернативных действий, которые должны приводить к достижению поставленных целей проекта разными путями
4. учет и анализ влияния неопределенностей характеристик альтернатив, определяющих их выбор, на эффект проекта

30. Управление проектными рисками включает в себя:

1. оценку рисков
3. реагирование на риски
2. контроль результатов реагирования
4. изменение рисков на начальном этапе

3 ТИПОВЫЕ ЗАДАНИЯ НА КОНТРОЛЬНУЮ РАБОТУ, КУРСОВУЮ РАБОТУ/КУРСОВОЙ ПРОЕКТ, РАСЧЕТНО-ГРАФИЧЕСКУЮ РАБОТУ

Данный вид контроля по дисциплине не предусмотрен учебным планом.

4 СВЕДЕНИЯ О ФОНДЕ ОЦЕНОЧНЫХ СРЕДСТВ И ЕГО СОГЛАСОВАНИИ

Фонд оценочных средств для аттестации по дисциплине «**Аудит информационной безопасности**» представляет собой компонент основной профессиональной образовательной программы специалитета по специальности **10.05.03 Информационная безопасность автоматизированных систем** (Специализация "Безопасность открытых информационных систем").

Старший преподаватель кафедры Информационной безопасности: А.А. Бабаева.

Фонд оценочных средств рассмотрен и одобрен методической комиссией института цифровых технологий (протокол №5 от 29.08.2024 г).

Председатель методической комиссии  О.С. Витренко