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)

«УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»

основной профессиональной образовательной программы специалитета
по специальности

10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специализация

«БЕЗОПАСНОСТЬ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ»

ИНСТИТУТ	цифровых технологий
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	Управление информационной безопасностью	*Знать:* автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; меры (компоненты) обеспечения безопасности компьютерных систем *Уметь:* определять критерии эффективности работы средств защиты информации; определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем *Владеть:* навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем

1.2 К оценочным средствам текущего контроля успеваемости относятся:

– тестовые задания открытого и закрытого типа с ключами правильных ответов.

К оценочным средствам для промежуточной аттестации относятся:

– экзаменационные задания по дисциплине, представленные в виде тестовых заданий закрытого и открытого типов с ключами правильных ответов.

Промежуточная аттестация по дисциплине проводится в форме зачета, который выставляется по результатам прохождения всех видов текущего контроля успеваемости. При необходимости тестовые задания закрытого и открытого типов могут быть использованы для проведения промежуточной аттестации.

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

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. Совокупность документов, определяющих управленческие и проектные решения в области защиты информации называется…

Эталонный ответ: политика информационной безопасности

2. Модель политики безопасности, выраженная точным, возможно математическим образом, включающим начальное состояние системы, способы перехода системы из одного состояния в другое и определение "безопасного" состояния системы называется…

Эталонный ответ: формальная модель политики безопасности

3. План реагирования на опасные ситуации, резервного копирования и последующих восстановительных процедур, являющийся частью программы защиты и обеспечивающий доступность основных ресурсов системы, и непрерывность обработки в кризисных ситуациях – это...

Эталонный ответ: план обеспечения непрерывной работы и восстановления функционирования.

4. Модель безопасности —

Эталонный ответ: описание требований безопасности к автоматизированной информационной системе. Обычно заключается в определении потоков информации, разрешенных в системе, и правил управления доступом к информации.

5. Неформальная модель нарушителя —

Эталонный ответ: описание вероятного нарушителя, включающее его потенциальные возможности и знания, время и место действия, необходимые усилия и средства для осуществления атаки и т.п.

6. Критерий аудита информационной безопасности организации –

Эталонный ответ: совокупность принципов, положений, требований и показателей действующих нормативных документов, относящихся к деятельности организации в области информационной безопасности.

7. Критерий обеспечения информационной безопасности организации –

Эталонный ответ: показатель, на основании которого оценивается степень достижения цели (целей) информационной безопасности организации.

8. Меры обеспечения информационной безопасности –

Эталонный ответ: совокупность действий, направленных на разработку и/или практическое применение способов и средств обеспечения информационной безопасности.

9. Мониторинг информационной безопасности организации –

Эталонный ответ: постоянное наблюдение за процессом обеспечения информационной безопасности в организации с целью установить его соответствие требованиям по информационной безопасности.

10 Нарушение информационной безопасности организации –

Эталонный ответ: случайное или преднамеренное неправомерное действие физического лица (субъекта, объекта) в отношении активов организации, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах, вызывающее негативные последствия (ущерб/вред) для организации.

11. Нарушитель информационной безопасности организации –

Эталонный ответ: физическое лицо или логический объект, случайно или преднамеренно совершивший действие, следствием которого является нарушение информационной безопасности организации.

12. Привилегии администратора -

Эталонный ответ: полный контроль над любой данной системой.

13. Атака, направленная на нарушение безопасности компьютерной системы, сети или устройства с намерением украсть данные, нарушить работу, нанести ущерб или получить несанкционированный доступ

Эталонный ответ: кибератака.

14. Метод защиты компьютеров, сетей, программ и данных от несанкционированного доступа или использования хакерами в целях эксплуатации.

Эталонный ответ: кибербезопасность.

15. Хакерская атака, в результате которой устройство добывает криптовалюту в дополнение к ее обычному использованию.

Эталонный ответ: криптоджекинг.

16. Вредоносная угроза группе или организации, исходящая от кого-либо внутри, например сотрудника, подрядчика или делового партнера, который владеет инсайдерской информацией о данных организации, компьютерных системах или мерах безопасности.

Эталонный ответ: инсайдерская угроза.

17. Метод получения пользовательской информации посредством мошеннических сообщений, нацеленных непосредственно на людей. Обычно это делается с помощью электронных писем, замаскированных под поступление из законного источника, но информация о цели возвращается фактическому источнику хакера.

Эталонный ответ: фишинг.

18. Система мероприятий защитных регулярных, направленных на обеспечение безопасности в соответствии с изменяющимися условиями среды внутренней и внешней –

Эталонный ответ: управление безопасностью.

19. Процесс выявления, контроля и минимизации или устранения рисков безопасности, оказывающих влияние на системы информационные, в рамках затрат допустимых -

Эталонный ответ: управление риском

20. Систематическая идентификация и менеджмент применяемых организацией бизнес-процессов и особенно взаимодействия таких процессов это

Эталонный ответ: процессный подход.

21. Система (организация, коллектив и т. п.), на которую направлены все виды управленческого воздействия с целью ее совершенствования, повышения качества функций и задач, успешного достижения запланированной цели (целей) это

Эталонный ответ: объект управления.

22. Совокупность сознательно и последовательно применяемых способов и приемов воздействия субъекта управления на объект управления посредством своей деятельности для достижения поставленной цели это

Эталонный ответ: метод управления.

23. Уровень зрелости СУИБ –

Эталонный ответ: степень способности системы управления информационной безопасностью достижения целей ИБ.

24. Деятельность, связанная с определением способности системы управления информационной безопасностью достижения целей ИБ -

Эталонный ответ: оценка зрелости СУИБ.

Тестовые задания закрытого типа:

1. Основные факторы, учитываемые при оценке рисков ИБ

- тяжесть возможных последствий

- вероятность происшествия

- квалификация персонала

- погодные условия

2. К внутренним угрозам безопасности объектов относятся

- негативные воздействия недобросовестных конкурентов

- отсутствие должной квалификации персонала по управлению объектом защиты

- преднамеренные и непреднамеренные действия персонала по нарушению безопасности

- преднамеренные и непреднамеренные действия заинтересованных структур и физических лиц

- неквалифицированная политика безопасности предприятия

3. «Дерево вариантов» используется в методике:

- FRAP

- CRAMM

- OCTAVE

- Risk Watch

4. Количество этапов внедрения системы менеджмента информационной безопасности

- 3

- 5

- 8

- 4

5. Метод оценки рисков на основе модели угроз и уязвимостей описывает:

- как производится выбор эффективных и экономически оправданных защитных мер, и средств для уменьшения или нейтрализации рисков

- как добросовестно выполняется и тщательно документируется оценка

- как производится построение модели информационной системы организации

- как анализируются все угрозы, действующие на информационную систему, и уязвимости, через которые возможна реализации угроз

6. Кто готовит План проведения аудита

- ведущий аудитор

- специалист ФСТЭК

- заказчик

- экспертный совет аудиторов

- исполнитель

7. Основными условиями принятия рисков ИБ являются:

- организация не может подобрать механизмы контроля

- стоимость реализации механизма контроля превышает потенциальные потери в случае осуществления риска

- стоимость реализации механизма контроля ниже потенциальных потерь в случае осуществления риска

- организация не хочет подбирать механизмы контроля

8. Выберите правильную последовательность событий в СМИБ

Планирование – Реализация – Оценка (Проверка) – Поддержка (Действие)

Планирование – Оценка (Проверка) — Поддержка (Действие) - Реализация

Оценка (Проверка) – Планирование – Поддержка (Действие) – Реализация

Поддержка (Действие) – Реализация – Планирование – Оценка (Проверка)

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

В данном разделе по учебному плану типовые задания на контрольную работу, курсовую работу/курсовой проект, расчётно-графическую работу не предусмотрены.

4 СВЕДЕНИЯ О ФОНДЕ ОЦЕНОЧНЫХ СРЕДСТВ И ЕГО СОГЛАСОВАНИИ

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

Разработчик – доцент кафедры «Информационная безопасность» — А.Г. Жестовский.

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

Председатель методической комиссии  О.С. Витренко