



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

УТВЕРЖДАЮ
Начальник УРОПС

Фонд оценочных средств
(приложение к программе практики)

ПРОИЗВОДСТВЕННАЯ ПРАКТИКА – ПРЕДИПЛОМНАЯ ПРАКТИКА

основной профессиональной образовательной программы высшего образования
программы специалитета по специальности

**10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
АВТОМАТИЗИРОВАННЫХ СИСТЕМ**

Специализация

«БЕЗОПАСНОСТЬ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ»

ИНСТИТУТ
РАЗРАБОТЧИК

Цифровых технологий
кафедра информационной безопасности

1 РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРАКТИКИ

Таблица 1 – Планируемые результаты, 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
<p>ПК-2: Способен разрабатывать проектные решения по защите информации в автоматизированных системах;</p> <p>ПК-4: Способен проводить анализ структурных и функциональных схем, защищённых автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем;</p> <p>ПК-5: Способен разрабатывать модели автоматизированных систем и подсистем безопасности автоматизированных систем;</p>	<p>ПК-2.4: Определяет структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации открытых информационных систем;</p> <p>ПК-4.3: Применяет меры по защите информации от основных угроз информации в автоматизированных системах и способы выявления потенциальных уязвимостей информационной безопасности автоматизированных систем;</p> <p>ПК-5.5: Формирует перечень мероприятий по разработке систем защиты информации автоматизированных систем;</p> <p>ПК-6.5: Анализирует</p>	<p>Преддипломная практика</p>	<p><u>Знать:</u></p> <ul style="list-style-type: none"> - технические характеристики, показатели качества ЭВМ и систем, методы их оценки и пути совершенствования; - источники и классификацию угроз информационной безопасности; - программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях; - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах. <p><u>Уметь:</u></p> <ul style="list-style-type: none"> - формировать перечень мероприятий по разработке систем защиты информации автоматизированных систем; - анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей систем защиты информации автоматизированных систем. <p><u>Владеть:</u></p> <ul style="list-style-type: none"> - навыками выборки меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы; - способностью к составлению плана распределения личного времени для выполнения задач на дипломное проектирование; - способностью определять структуру системы защиты информации автоматизированной системы в соответствии с

Код и наименование компетенции	Индикаторы достижения компетенции	Дисциплина	Результаты обучения (владения, умения и знания), соотнесенные с компетенциями/индикаторами достижения компетенции
ПК-6: Способен к анализу защищённости информационной инфраструктуры автоматизированной системы	программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей систем защиты информации автоматизированных систем		требованиями нормативных правовых документов в области защиты информации открытых информационных систем. Должен приобрести опыт: - в выборке мер защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы; - определения структуры системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации открытых информационных систем.

2 ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ И КРИТЕРИИ ОЦЕНИВАНИЯ

2.1 К оценочным средствам для промежуточной аттестации, проводимой в форме дифференцированного зачета (зачет с оценкой), относятся:

- отчет по практике;
- тестовые задания закрытого и открытого типов.

2.2 Критерии оценки результатов прохождения практики

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	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

Система оценок Критерий	2	3	4	5
	0-40%	41-60%	61-80 %	81-100 %
	«неудовлетворительно»	«удовлетворительно»	«хорошо»	«отлично»
	«не зачтено»	«зачтено»		
	некоторые из которых может связывать между собой)			
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	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом, понимает основы	Не только владеет алгоритмом и понимает его основы, но и предлагает новые решения в рамках поставленной задачи

Система оценок Критерий	2	3	4	5
	0-40%	41-60%	61-80 %	81-100 %
	«неудовлетворительно»	«удовлетворительно»	«хорошо»	«отлично»
	«не зачтено»	«зачтено»		
	алгоритм, допускает ошибки		предложенного алгоритма	

2.4 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.

3 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Компетенция ПК-2: Способен разрабатывать проектные решения по защите информации в автоматизированных системах.

Индикатор ПК-2.4: Определяет структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации открытых информационных систем.

Тестовые задания открытого типа

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

2. Правовая форма защиты информации – это ...

3. Верификация и подтверждение правильности – это...

Тестовые задания закрытого типа

1. Укажите соответствие количества документов, прилагаемых к заявке на сертификацию

1	технические условия	а	2 экз.
2	техническое задание (в случае, если планируется проведение сертификации средства защиты информации на соответствие требованиям по безопасности информации, изложенным в техническом задании)	б	2 экз.

3	задание по безопасности (в случае необходимости его разработки в соответствии с требованиями по безопасности информации)	в	2 экз.
4	формуляр (паспорт) на средство защиты информации	г	1 экз.
5	договор с лицом (лицами), обладающим (обладающими) исключительными правами на средство защиты информации, о предоставлении заявителю права на сертификацию, эксплуатацию или производство средства защиты информации, а также на техническую поддержку средства защиты информации	д	1 экз.

2. Укажите последовательность действий заявителя при намерении сертифицировать средство защиты информации

1	а	относит планируемое к сертификации средство защиты информации к одному из типов средств защиты информации, установленных требованиями по безопасности информации и подлежащих сертификации в системе сертификации ФСТЭК России
2	б	определяет требования по безопасности информации, на соответствие которым планируется проведение сертификации средства защиты информации
3	в	готовит конструкторскую, программную и эксплуатационную документацию на средство защиты информации
4	г	выбирает для проведения сертификационных испытаний средства защиты информации аккредитованную ФСТЭК России в соответствующей области аккредитации испытательную лабораторию, согласовывает с ней возможность и сроки проведения сертификационных испытаний

3. Укажите последовательность сертификационных испытаний

1	а	проведение испытаний отобранного образца (образцов) средства защиты информации, предусматривающих оценку соответствия параметров и характеристик (функций безопасности информации) средства защиты информации требованиям по безопасности информации
2	б	проверку организации технической поддержки средства защиты информации, предусматривающую оценку соответствия работ (услуг) по технической поддержке средства защиты информации в ходе его эксплуатации, проводимых (предоставляемых) заявителем, требованиям по безопасности информации
3	в	проверку организации производства средства защиты информации, предусматривающую оценку соответствия работ по изготовлению средства защиты информации с целью подтверждения неизменности параметров и характеристик (функций безопасности информации) образцов серийно производимого средства защиты информации требованиям по безопасности информации (при сертификации производства средства защиты информации)

Компетенция ПК-4: Способен проводить анализ структурных и функциональных схем, защищённых автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем.

Индикатор ПК-4.3: Применяет меры по защите информации от основных угроз информации в автоматизированных системах и способы выявления потенциальных уязвимостей информационной безопасности автоматизированных систем.

Тестовые задания открытого типа

1. 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...

2. Слабость в системных средствах защиты, вызванная ошибками или слабостями в процедурах, проекте, реализации, внутреннем контроле системы, которая может быть использована для нарушения системной политики безопасности называется...

3. Фактор опасности – это...

4. Программно-аппаратное устройство, обеспечивающее корректировку ошибок идентификации, переданных с удаленных терминалов по каналам связи называется...

Тестовые задания закрытого типа

1. Укажите соответствие действий участников сертификации средств защиты информации

1	Федеральный орган по сертификации	а	организует проведение сертификации средств защиты информации, разрабатывает и устанавливает в пределах своей компетенции требования по безопасности информации к средствам защиты информации,
2	Органы по сертификации	б	оформляют сертификаты соответствия средств защиты информации требованиям по безопасности информации (далее - сертификат соответствия)
3	Испытательные лаборатории	в	проводят сертификационные испытания средств защиты информации и по их результатам оформляют технические заключения и протоколы.
4	Изготовители средств защиты информации	г	разрабатывают и (или) производят средства защиты информации в соответствии с требованиями по безопасности информации.

2. Укажите соответствие схемы сертификации различных средств защиты информации

1	для единичного образца средства защиты информации	а	проведение испытаний образца средства защиты информации и проверки организации его технической поддержки
2	для партии средства защиты информации	б	проведение испытаний выборки образцов средства защиты информации и проверки организации его технической поддержки

3	для серийного производства средства защиты информации	в	проведение испытаний выборки образцов средства защиты информации и проверки организации его производства и технической поддержки
---	---	---	--

3. Укажите последовательность действий исполнителя при проведении сертификации средств защиты информации

1	а	подача заявки на сертификацию
2	б	принятие решения о проведении сертификации средства защиты информации
3	в	сертификационные испытания средства защиты информации
4	г	оформление экспертного заключения по результатам сертификации средства защиты информации и проекта сертификата соответствия
5	д	выдача (отказ в выдаче) сертификата соответствия
6	е	предоставление дубликата сертификата соответствия

4. Укажите последовательность действий исполнителя при проведении сертификации средств защиты информации

1	а	маркирование средств защиты информации
2	б	внесение изменений в сертифицированное средство защиты информации
3	в	переоформление сертификата соответствия
4	г	продление срока действия сертификата соответствия
5	д	приостановление действия сертификата соответствия
6	е	прекращение действия сертификата соответствия

Компетенция ПК-5: Способен разрабатывать модели автоматизированных систем и подсистем безопасности автоматизированных систем.

Индикатор ПК-5.5: Формирует перечень мероприятий по разработке систем защиты информации автоматизированных систем.

Тестовые задания открытого типа

1. 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...

2. Модель Белла-Лападула - это...

Тестовые задания закрытого типа

1. Укажите соответствие действий Заявителя и Уполномоченной организацией при подаче документов на объект информатизации

1	Заявитель	а	Приказ (распоряжение) «О назначении комиссии по категорированию и классификации объектов информатизации»
---	-----------	---	--

2	Уполномоченная организация	б	Предписание на эксплуатацию ОТСС объекта информатизации и протокол специальных исследований (СИ).
3	Заявитель	в	Акт категорирования объекта информатизации
4	Заявитель	г	Акт классификации АС в составе ОИ
5	Заявитель	д	Технический паспорт объекта информатизации (должен содержать схему ОИ с указанием границ контролируемой зоны, схему прокладки линий передачи данных, схемы и характеристики системы электропитания и заземления)
6	Уполномоченная организация	е	Заключение по результатам специальной проверки ТС иностранного производства
7	Уполномоченная организация	ж	Протокол измерения параметров заземлителя ТСС ОИ

2. Укажите последовательность действий заявителя при проведении предаттестационных мероприятий

1	а	Определяется перечень информации, подлежащей защите
2	б	Определяется степень конфиденциальности (секретности) обрабатываемой информации
3	в	Определяется категория объекта с оформлением акта категорирования ОТСС
4	г	Определяется класс защищенности АС с оформлением акта классификации АС по требованиям защиты

Компетенция ПК-6: Способен к анализу защищённости информационной инфраструктуры автоматизированной системы.

Индикатор ПК-6.5: Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей систем защиты информации автоматизированных систем.

Тестовые задания открытого типа

1. Специальная программа, входящая в комплект программного обеспечения и предназначенная для защиты информации, называется...
2. Защищенная информационная система – это...

Тестовые задания закрытого типа

1. Укажите соответствие действий Заявителя и Аттестующей организацией при подаче документов на объект информатизации

1	Заявитель	а	Разрешительная система доступа к информационным ресурсам АС
2	Аттестующая организация	б	Программа и методика аттестационных испытаний
3	Заявитель	в	Описание технологического процесса обработки информации

4	Заявитель	г	Данные по уровню подготовки кадров обеспечивающих защиту информации
5	Заявитель	д	Технологические инструкции пользователям и администратору безопасности АС
6	Аттестующая организация	е	Заключение по результатам аттестационных испытаний
7	Аттестующая организация	ж	Аттестат соответствия
8	Заявитель	з	Приказ о вводе ОИ в эксплуатацию

2. Укажите последовательность определения класса защищенности государственной информационной системы

1	а	степень возможного ущерба для обладателя информации (заказчика) и (или) оператора от нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение),
2	б	целостность (неправомерные уничтожение или модифицирование)
3	в	доступность (неправомерное блокирование) информации).

4 ТИПОВЫЕ ЗАДАНИЯ НА КОНТРОЛЬНУЮ РАБОТУ, КУРСОВУЮ РАБОТУ/ КУРСОВОЙ ПРОЕКТ

Данный вид контроля по производственной практике – преддипломной практике работе не предусмотрен учебным планом.

5 СВЕДЕНИЯ О ФОНДЕ ОЦЕНОЧНЫХ СРЕДСТВ И ЕГО СОГЛАСОВАНИИ

Фонд оценочных средств для аттестации по производственной практике – преддипломной практике представляет собой компонент основной профессиональной образовательной программы специалитета по специальности подготовки 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).

Фонд оценочных средств актуализирован. Изменения, дополнения рассмотрены и одобрены на заседании кафедры информационной безопасности 20.03.2023 г. (протокол № 6).

Заведующая кафедрой



Н.Я. Великите