



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)

УЧЕБНАЯ ПРАКТИКА – ОЗНАКОМИТЕЛЬНАЯ 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>УК-6: Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни;</p> <p>ПК-2: Способен разрабатывать проектные решения по защите информации в автоматизированных системах;</p> <p>ПК-3: Способен выявлять основные угрозы безопасности информации в автоматизированных системах</p>	<p>УК-6.3: Анализирует требования рынка труда к личностным и профессиональным навыкам. Производит оценку уровня саморазвития в различных сферах профессиональной деятельности;</p> <p>ПК-2.2: Применяет действующую законодательную базу в области обеспечения информационной безопасности;</p> <p>ПК-3.3: Обеспечивает выявление основных угроз безопасности информации с помощью типовых программных средств</p>	<p>Ознакомительная практика</p>	<p><u>Знать:</u></p> <ul style="list-style-type: none"> - сущность и понятие информации, информационной безопасности и характеристику ее составляющих; - правовые основы организации защиты государственной тайны и конфиденциальной информации; - терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем; - принципы формирования политики информационной безопасности в автоматизированных системах. <p><u>Уметь:</u></p> <ul style="list-style-type: none"> - применять действующую законодательную базу в области обеспечения информационной безопасности; - классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; - осуществлять сбор, обработку, анализ и систематизацию научно-технической информации с применением современных информационных технологий. <p><u>Владеть:</u></p> <ul style="list-style-type: none"> - навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; - навыками работы с офисными приложениями; - навыками обеспечения безопасности информации с помощью типовых программных средств. <p>Должен приобрести опыт:</p> <ul style="list-style-type: none"> - работы с офисными приложениями; - обеспечение безопасности информации с помощью типовых программных средств.

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 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,	Не может делать научно корректных выводов из имеющихся у него	В состоянии осуществлять научно корректный	В состоянии осуществлять систематический и научно	В состоянии осуществлять систематический и научно-

Система оценок Критерий	2	3	4	5
	0-40%	41-60%	61-80 %	81-100 %
	«неудовлетворительно»	«удовлетворительно»	«хорошо»	«отлично»
	«не зачтено»	«зачтено»		
процесса, объекта	сведений, в состоянии проанализировать только некоторые из имеющихся у него сведений	анализ предоставленной информации	корректный анализ предоставленной информации, вовлекает в исследование новые релевантные задаче данные	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

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 УК-6: Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни.

Индикатор УК-6.3: Анализирует требования рынка труда к личностным и профессиональным навыкам. Производит оценку уровня саморазвития в различных сферах профессиональной деятельности.

Тестовые задания открытого типа

1. Умение осуществлять поиск, преобразование и передачу информации средствами информационно-коммуникационных технологий и выполнять различные социальные роли в группе и коллективе -

2. Самореализация - это ...

3. Государственная тайна –

Тестовые задания закрытого типа

1. Укажите соответствие действий исполнителя при формировании основных документов по результатам исполнения работ на этапе внедрения системы защиты информации:

	Действие		Документ
1	Установка и настройка средств защиты информации	а	Акт установки средств защиты информации
2	Внедрение организационных мер, разработка организационно-распорядительных документов	б	Документы по регламентации правил по эксплуатации и вывода из эксплуатации системы защиты информации
3	Выявление и анализ	в	Протокол контроля уязвимостей программного обеспечения и технических средств
4	Испытания и опытная эксплуатация системы защиты информации уязвимостей	г	Протоколы контроля оценки эффективности средств и оценки защищенности информации

2. Укажите последовательность действий исполнителя при проведении аттестации информационных систем по требованиям безопасности информации

1	а	Подача и рассмотрение заявки на аттестацию.
2	б	Предварительное ознакомление с аттестуемым объектом (при необходимости).
3	в	Разработка программы и методики аттестационных испытаний.

4	г	Проведение аттестационных испытаний объекта.
5	д	Оформление, регистрация и выдача аттестата соответствия.

3. Укажите последовательность действий при создании системы защиты информации

1	а	Формирование требований к системе защиты информации (предпроектный этап).
2	б	Разработка системы защиты информации (этап проектирования).
3	в	Внедрение системы защиты информации (этап установки, настройки, испытаний).
4	г	Подтверждение соответствия системы защиты информации (этап оценки).

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

Индикатор ПК-2.2: Применяет действующую законодательную базу в области обеспечения информационной безопасности.

Тестовые задания открытого типа

1. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственниками информации называется ...

- 2. Правовая защита – это ...
- 3. Персональные данные –

Тестовые задания закрытого типа

1. Укажите соответствие действий исполнителя при формировании основных документов по результатам исполнения работ на этапе формирования требований к системе защиты информации:

	Действие		Документ
1	Принятие решения о необходимости защиты информации	а	Локальный нормативный правовой акт, определяющий необходимость создания системы защиты информации
2	Классификация по требованиям защиты информации (по уровню защищенности информации)	б	Акт классификации по требованиям безопасности информации
3	Определение актуальных угроз безопасности информации	в	Частная модель угроз безопасности информации
4	Определение требований к системе защиты информации	г	ТЗ на создание системы защиты информации с указанием требований к мерам и средствам защиты информации

2. Укажите последовательность действий исполнителя при **реагировании на инциденты**

1	а	подготовка
2	б	обнаружение
3	в	сдерживание
4	г	исправление
5	д	восстановление
6	е	улучшение

3. Укажите последовательность действий исполнителя при формировании основных документов по результатам исполнения работ на этапе внедрения системы защиты информации

1	а	Установка и настройка средств защиты информации
2	б	Внедрение организационных мер защиты информации, в том числе, разработка документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в ходе эксплуатации объекта
3	в	Выявление и анализ уязвимостей программных и технических средств, принятие мер по их устранению
4	г	Испытания и опытная эксплуатации системы защиты информации

Компетенция ПК-3: Способен выявлять основные угрозы безопасности информации в автоматизированных системах.

Индикатор ПК-3.3: Обеспечивает выявление основных угроз безопасности информации с помощью типовых программных средств.

Тестовые задания открытого типа

1. Обобщенный параметр, учитывающий ценность ресурса, уровень угрозы и степень уязвимости, называется ...
2. Угроза информации – это ...
3. Мониторинг событий ИБ –

Тестовые задания закрытого типа

1. Укажите соответствие действий оператора при администрировании системы защиты информации, выявление инцидентов и реагирование на них, управление конфигурацией объекта и его системой защиты информации, контроль за обеспечением необходимого уровня защищенности информации

1	Заявители	а	осуществляют эксплуатацию объекта информатизации в соответствии с требованиями безопасности информации, а также условиями и ограничениями, установленными эксплуатационной документацией на систему защиты информации, и аттестатом соответствия
2	Заявители	б	извещают орган по аттестации (организацию), выдавший аттестат соответствия, о всех изменениях в информационных технологиях, составе и размещении средств и систем, условиях их эксплуатации, которые могут повлиять на эффективность системы защиты информации
3	Заявители	в	предоставляют необходимые документы и условия для осуществления контроля и надзора за соблюдением порядка аттестации и за эксплуатацией аттестованного объекта информатизации
4	Органы по аттестации	г	Органы по аттестации
5	Органы по аттестации	д	отменяют и приостанавливают действие выданных этим органом (организацией) аттестатов соответствия
6	Органы по аттестации	е	проводят на договорной основе оценку эффективности средств защиты информации и оценку защищенности информации от несанкционированного доступа

2. Укажите последовательность действий исполнителя при формировании основных документов по результатам исполнения работ на этапе разработки системы защиты информации

		Документ
1	а	Технический проект (рабочая документация) на создание системы защиты информации
2	б	Описание структуры системы защиты информации.
3	в	Технический паспорт с указанием наименования, состава и мест установки аппаратных и программных средств
4	г	Перечень параметров настройки средств защиты информации.
5	д	Правила эксплуатации средств защиты информации.

3. Укажите последовательность действий при подаче и рассмотрении заявки на аттестацию объекта информатизации

1	а	Заявителем выбирается исполнитель работ по аттестации объекта информатизации (организация-лицензиат по технической защите конфиденциальной информации)
---	---	--

2	б	Заявителем направляется исполнителю заявка на проведение аттестации с исходными данными на аттестуемый объект
3	в	Исполнителем рассматривается заявка, принимается решение о порядке аттестации, готовятся договорные документы на оказание услуг по аттестации объекта информатизации

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

Данный вид контроля по учебной практике – ознакомительной практике не предусмотрен учебным планом.

5 СВЕДЕНИЯ О ФОНДЕ ОЦЕНОЧНЫХ СРЕДСТВ И ЕГО СОГЛАСОВАНИИ

Фонд оценочных средств для аттестации по учебной практике – ознакомительной 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