



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

УТВЕРЖДАЮ
И.о. директора института

Фонд оценочных средств
(приложение к рабочей программе модуля)
**«ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»**

основной профессиональной образовательной 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 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
<p>ОПК-5: Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации</p>	<p>Организационное и правовое обеспечение информационной безопасности</p>	<p>Знать: понятие и виды защищаемой информации по законодательству РФ; терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем; принципы формирования политики информационной безопасности в автоматизированных системах, Уметь: применять действующую законодательную базу в области обеспечения информационной безопасности; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности Владеть: навыками работы с нормативными правовыми актами; навыками работы с технической документацией на ЭВМ и вычислительные системы; навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках;</p>
<p>ОПК-6: Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю</p>		<p>Знать: правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; основные отечественные и зарубежные стандарты в области информационной безопасности; законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации Уметь: применять действующую законодательную базу в области обеспечения информационной безопасности; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности Владеть: навыками разработки и</p>

		использования методическими материалами по регламентации системы организационной защиты информации.
--	--	---

1.2 К оценочным средствам текущего контроля успеваемости относятся:

- тестовые задания открытого и закрытого типов;

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	2	3	4	5
	0-40%	41-60%	61-80 %	81-100 %
Критерий	«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 полной 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

Система оценок Критерий	2	3	4	5
	0-40%	41-60%	61-80 %	81-100 %
	«неудовлетворительно»	«удовлетворительно»	«хорошо»	«отлично»
	«не зачтено»	«зачтено»		
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-5: Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации

Тестовые задания открытого типа:

1. Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций –

Эталонный ответ: автоматизированная система

2. Администратор безопасности АС –

Эталонный ответ: субъект доступа, ответственный за защиту АС от несанкционированного доступа к информации;

3. Комплекс организационных и технических мероприятий, в результате которых подтверждается соответствие системы защиты информации объекта информатизации требованиям безопасности информации

Эталонный ответ: аттестация объектов информатизации

4. Безопасность информации –

Эталонный ответ: состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность;

5. Технические средства и системы, не предназначенные для передачи, обработки и хранения секретной информации, устанавливаемые совместно с основными техническими средствами и системами

Эталонный ответ: вспомогательные технические средства и системы

6. Лицо, самостоятельно и по своему усмотрению определяющее порядок использования сайта в сети "Интернет", в том числе порядок размещения информации на таком сайте

Эталонный ответ: владелец сайта в сети "Интернет"

7. Зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель

Эталонный ответ: документированная информация

8. Доменное имя –

Эталонный ответ: обозначение символами, предназначенное для адресации сайтов в сети "Интернет" в целях обеспечения доступа к информации, размещенной в сети "Интернет";

9. Доступ к информации (доступ)

Эталонный ответ: ознакомление с информацией, ее обработка; в частности, копирование, модификация или уничтожение информации;

10. Федеральная государственная информационная система, порядок использования которой устанавливается Правительством Российской Федерации, и которая обеспечивает в случаях, предусмотренных законодательством Российской Федерации, санкционированный доступ к информации, содержащейся в информационных системах

Эталонный ответ: единая система идентификации и аутентификации

11. Защита информации –

Эталонный ответ: деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;

12. Отдельные документы и отдельные массивы документов, содержащиеся в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах), а также машинные носители информации (жесткие магнитные диски, гибкие магнитные диски, оптические диски и т.п.)

Эталонный ответ: информационные ресурсы

Тестовые задания закрытого типа:

1). К правовым методам, обеспечивающим информационную безопасность, относятся:

1. Разработка аппаратных средств обеспечения правовых данных
2. Разработка и установка во всех компьютерных правовых сетях журналов учета действий

3. Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:

1. Хищение жестких дисков, подключение к сети, инсайдерство

2. Перехват данных, хищение данных, изменение архитектуры системы

3. Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:

1. Персональная, корпоративная, государственная

2. Клиентская, серверная, сетевая

3. Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:

1. несанкционированного доступа, воздействия в сети
2. инсайдерства в организации
3. чрезвычайных ситуаций

5) Основные объекты информационной безопасности:

1. **Компьютерные сети, базы данных**
2. Информационные системы, психологическое состояние пользователей
3. Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:

1. Искажение, уменьшение объема, перекодировка информации
2. Техническое вмешательство, выведение из строя оборудования сети
3. **Потеря, искажение, утечка информации**

7) Основными субъектами информационной безопасности являются:

1. руководители, менеджеры, администраторы компаний
2. **органы права, государства, бизнеса**
3. сетевые базы данных, фаерволлы

ОПК-6: Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

Тестовые задания открытого типа:

1. Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя

Эталонный ответ: конфиденциальность информации

2. Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам

Эталонный ответ: обладатель информации

3. Совокупность операций сбора, накопления, ввода, вывода, приема, передачи, записи, хранения, регистрации, уничтожения, преобразования, отображения, осуществляемых над информацией

Эталонный ответ: обработка информации

4. Совокупность действий, направленных на применение организационных мер и программно-технических способов защиты информации на объекте информатизации

Эталонный ответ: организационно-технические мероприятия по обеспечению защиты информации

5. Гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных

Эталонный ответ: оператор информационной системы

6. Предоставление информации –

Эталонный ответ: действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц

7. Распространение информации –

Эталонный ответ: действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

8. Совокупность требований, правил, организационных, технических и иных мер, направленных на сохранность сведений, составляющих государственную тайну

9. Эталонный ответ: режим секретности

10. Помещение, в котором проводятся секретные работы и/или хранятся в нерабочее время носители сведений, составляющих государственную тайну

Эталонный ответ: режимное помещение

11. Совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети "Интернет" по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети "Интернет"

Эталонный ответ: сайт в сети "Интернет"

12. Секретная информация –

Эталонный ответ: информация, содержащие сведения, отнесенные к государственной тайне

13. Электронное сообщение –

Эталонный ответ: информация, переданная или полученная пользователем информационно-телекоммуникационной сети

14. Документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах

Эталонный ответ: электронный документ

Тестовые задания закрытого типа:

- 1) По доступности информация классифицируется на
- 1. открытую информацию и государственную тайну**
 2. конфиденциальную информацию и информацию свободного доступа
 3. информацию с ограниченным доступом и общедоступную информацию
- 2) К конфиденциальной информации относятся документы, содержащие
- 1. государственную тайну**
 2. законодательные акты
 3. "ноу-хау"
 4. сведения о золотом запасе страны
- 3) Запрещено относить к информации ограниченного доступа
1. информацию о чрезвычайных ситуациях
 2. информацию о деятельности органов государственной власти
 3. документы открытых архивов и библиотек
 - 4. все, перечисленное в остальных пунктах**
- 4) К конфиденциальной информации не относится
1. коммерческая тайна
 2. персональные данные о гражданах
 3. государственная тайна
 - 4. "ноу-хау"**
- 5) Согласно ст.132 ГК РФ интеллектуальная собственность это
1. информация, полученная в результате интеллектуальной деятельности индивида
 2. литературные, художественные и научные произведения
 3. изобретения, открытия, промышленные образцы и товарные знаки

4. исключительное право гражданина или юридического лица на результаты интеллектуальной деятельности

б) Интеллектуальная собственность включает права, относящиеся к

1. литературным, художественным и научным произведениям, изобретениям и открытиям

2. всему, указанному в остальных пунктах

3. промышленным образцам, товарным знакам, знакам обслуживания, фирменным наименованиям и коммерческим обозначениям

4. исполнительской деятельности артиста, звукозаписи, радио- и телепередачам

7). Формы защиты интеллектуальной собственности -

1. авторское, патентное право и коммерческая тайна

2. интеллектуальное право и смежные права

3. коммерческая и государственная тайна

4. гражданское и административное право

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 «Организационное и правовое обеспечение информационной безопасности» 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