



Министерство науки  
и высшего образования РФ  
ФГБОУ ВО «НИУ «МЭИ»  
Институт дистанционного  
и дополнительного образования



**ОЦЕНОЧНЫЕ И МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ КОНТРОЛЯ  
ОСВОЕНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ  
ДОПОЛНИТЕЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ  
повышения квалификации  
«Организация и технологии защиты информации: новое в отрасли»,**

**Текущий контроль**

Текущий контроль проводится в соответствии с характеристиками контрольных заданий и представлен в табл. 1.

Таблица 1

Характеристика заданий текущего контроля

Наименование дисциплины (модуля)	Форма контроля/наименование контрольной точки	Пример задания	Критерии оценки
<i>Не предусмотрено</i>			

**Промежуточная аттестация**

Промежуточная аттестация по программе проводится в форме зачета, экзамена или отчета о стажировке в соответствии с учебным планом. Характеристика заданий представлена в табл. 2.

Таблица 2

Характеристика заданий промежуточной аттестации

Наименование дисциплины (модуля)	Пример задания	Критерии оценки
Актуальное правовое и нормативное регулирование информационной безопасности	Не предусмотрено	Не предусмотрено
Управление информационной безопасностью	Не предусмотрено	Не предусмотрено
Менеджмент рисков	Не предусмотрено	Не предусмотрено

информационной безопасности		
Компьютерная безопасность	Не предусмотрено	Не предусмотрено
Современные аспекты безопасности информационных технологий	Не предусмотрено	Не предусмотрено
Образовательные и профессиональные стандарты по защите информации	Не предусмотрено	Не предусмотрено
Методика практической подготовки специалистов в сфере информационной безопасности	Не предусмотрено	Не предусмотрено

### Итоговая аттестация

Итоговая аттестация по программе проводится в форме *итогового зачета*. Характеристика заданий представлена в табл. 3.

Таблица 3

Характеристика заданий итоговой аттестации

Вид контроля	Краткая характеристика задания	Критерии оценки
Итоговая аттестация	<p>- <b>На какую информацию распространяются положения ФЗ «О коммерческой тайне»? (указать)</b></p> <p>а) на <u>информацию, составляющую коммерческую тайну</u>, кроме информации в электронном виде;</p> <p>б) на всю информацию ограниченного доступа;</p> <p>с) на <u>информацию, составляющую коммерческую тайну</u>, независимо от вида носителя, на котором она зафиксирована.</p> <p>- <b>Кто является обладателем информации, составляющей коммерческую тайну? (указать)</b></p> <p>а) лицо, самостоятельно</p>	<p><i>Оценка:</i> зачтено  <i>Описание характеристики выполнения знания:</i> Оценка «зачтено» заслуживает слушатель, обнаруживший всестороннее, систематическое и глубокое знание учебного и нормативного материала, умеющий свободно выполнять задания, предусмотренные программой.</p> <p><i>Оценка:</i> не зачтено  <i>Описание характеристики выполнения знания:</i> Оценка «не зачтено» выставляется слушателю, обнаружившему пробелы в знаниях основного учебного материала, допускающему принципиальные ошибки в выполнении предусмотренных программой</p>

	<p>создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;</p> <p>b) лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны;</p> <p>c) лицо, которое получило доступ к информации, составляющей коммерческую тайну, и владеет этой информацией на законном основании.</p> <p>- <b>Что такое доступ к информации, составляющей коммерческую тайну?</b></p> <p>d) ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации;</p> <p>e) процедура оформления права граждан на ознакомление со сведениями, составляющими коммерческую тайну, а предприятий, учреждений и организаций - на проведение работ с использованием таких сведений;</p> <p>f) ознакомление юридических лиц, индивидуальных предпринимателей и органов государственной власти с информацией, составляющей коммерческую тайну при условии сохранения конфиденциальности этой информации;</p> <p>g) ознакомление определенных лиц с информацией, составляющей коммерческую тайну, на основании</p>	заданий.
--	--	----------

	<p>федерального законодательства при условии сохранения конфиденциальности этой информации.</p> <p>- <b>Какую ответственность несет работник в случае неосторожного разглашения информации, составляющей коммерческую тайну при отсутствии в действиях такого работника состава преступления?</b></p> <p>a) административную; b) дисциплинарную; c) гражданско-правовую; d) уголовную; e) не несет ответственности.</p> <p>- <b>В отношении каких сведений не может быть установлен режим коммерческой тайны? (указать)</b></p> <p>a) в отношении сведений, перечисленных в ФЗ «О коммерческой тайне» и сведений обязательность раскрытия, которых или недопустимость ограничения доступа, к которым установлена иными федеральными законами; b) в отношении сведений, составляющих государственную тайну, используемых в деятельности коммерческого предприятия; c) в отношении сведений, которые не имеют действительной или потенциальной коммерческой ценности, в силу неизвестности их третьим лицам.</p> <p>- <b>Как осуществляется доступ работника к информации, составляющей коммерческую тайну? (указать)</b></p> <p>a) только с его согласия; b) по распоряжению руководителя; c) в соответствии с трудовыми обязанностями;</p>	
--	--	--

	<p>d) с его согласия, если это не предусмотрено его трудовыми обязанностями.</p> <p>- <b>Какую ответственность несет работник в случае умышленного разглашения информации, составляющей коммерческую тайну при отсутствии в действиях такого работника состава преступления? (указать)</b></p> <p>f) административную;</p> <p>g) дисциплинарную;</p> <p>h) гражданско-правовую;</p> <p>i) уголовную;</p> <p>j) не несет ответственности.</p> <p>- <b>Что такое передача к информации, составляющей коммерческую тайну? (указать)</b></p> <p>a) передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций;</p> <p>b) передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности;</p> <p>c) передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем по запросу судов, органов предварительного следствия, органов дознания по делам, находящимся в их производстве, в порядке и на</p>	
--	--	--

	<p>основаниях, которые предусмотрены законодательством Российской Федерации.</p> <ul style="list-style-type: none"><li>- <b>Международная организация по стандартизации имеет аббревиатуру (указать)</b><ul style="list-style-type: none"><li>a) ISO;</li><li>b) IEC;</li><li>c) ИСО;</li><li>d) 3;</li><li>e) 1 и 3.</li></ul></li><li>- <b>Какой стандарт из семейства 27000 является «Руководством по аудиту»? (указать)</b><ul style="list-style-type: none"><li>a) 27005</li><li>b) 27006</li><li>c) 27007</li><li>d) 27011</li><li>e) 27031</li></ul></li><li>- <b>Стандартизацией в какой области не занимается ISO? (указать)</b><ul style="list-style-type: none"><li>a) занимается всеми</li><li>b) криптография</li><li>c) электротехника и электроника</li><li>d) техническая защита информации</li></ul></li><li>- <b>Какие процессы не относятся к идентификации рисков согласно требованиям стандарта 27001? (указать)</b><ul style="list-style-type: none"><li>a) Идентификация объектов;</li><li>b) Идентификация активов;</li><li>c) Идентификация угроз;</li><li>d) Идентификация уязвимостей;</li><li>e) Идентификация последствий воздействия;</li></ul></li><li>- <b>Как называется Федеральный закон, определяющий правовые основы стандартизации в РФ? (указать)</b><ul style="list-style-type: none"><li>1. О персональных данных;</li><li>2. Об информации, ИТ и защите информации;</li><li>3. О стандартизации;</li></ul></li></ul>	
--	--	--

	<p>4. О техническом регулировании;</p> <p>- <b>Какие процессы не относятся к идентификации рисков согласно требованиям стандарта 27001? (указать)</b></p> <ol style="list-style-type: none"> <li>1. Идентификация объектов;</li> <li>2. Идентификация активов;</li> <li>3. Идентификация угроз;</li> <li>4. Идентификация уязвимостей;</li> <li>5. Идентификация последствий воздействия;</li> </ol> <p>- <b>Положительная обратная связь означает, что (указать)</b></p> <ol style="list-style-type: none"> <li>1. входной и выходной сигналы равны</li> <li>2. при увеличении входного сигнала увеличивается выходной</li> <li>3. при увеличении входного сигнала уменьшается выходной</li> <li>4. при уменьшении входного сигнала увеличивается выходной сигнал</li> </ol> <p>- <b>Основные принципы системного подхода (отметить лишний)</b></p> <ol style="list-style-type: none"> <li>1. принцип конечной цели</li> <li>2. принцип единства</li> <li>3. принцип развития</li> <li>4. принцип самостоятельности</li> </ol> <p>- <b>К внутренним системообразующим факторам не относится (указать)</b></p> <ol style="list-style-type: none"> <li>1. фактор взаимозаменяемости</li> <li>2. фактор саморегулирования</li> <li>3. фактор саморазрушения</li> <li>4. фактор компенсации</li> </ol> <p>- <b>С чего начинается описание системы (указать)</b></p> <ol style="list-style-type: none"> <li>1. с выделения объекта среди других и представление его как системы</li> <li>2. с определения классификационных характеристик системы</li> <li>3. с определение целей, задач и назначения (функций) системы</li> <li>4. с установление связей системы с другими системами</li> </ol>	
--	--	--

	<p>- <b>Основные принципы управления: (указать)</b></p> <ol style="list-style-type: none"> <li>1. планирование, организация, и контроль</li> <li>2. организация, планирование, координация</li> <li>3. организация, контроль, координация, мотивация</li> <li>4. планирование, организация, координация, мотивация и контроль</li> </ol> <p>- <b>Первой фазой проектирования систем является (указать)</b></p> <ol style="list-style-type: none"> <li>1. оценка</li> <li>2. формирование стратегии или планирования</li> <li>3. реализация</li> <li>4. поиск и разработка вариантов</li> </ol> <p>- <b>Основные шаги в процессе принятия решений (указать лишний):</b></p> <ol style="list-style-type: none"> <li>1. постановка цели решения</li> <li>2. установление критериев решения</li> <li>3. разделение критериев (ограничения/желательные характеристики)</li> <li>4. выработка альтернатив</li> <li>5. принятие альтернатив</li> <li>6. сравнение альтернатив</li> <li>7. определение риска</li> <li>8. оценка риска (вероятность/серьезность)</li> <li>9. принятие решения</li> </ol> <p>- <b>Выходным элементом системы называется результат (указать)</b></p> <ol style="list-style-type: none"> <li>1. внутреннего функционирования системы</li> <li>2. взаимодействия внутренних структур систем</li> <li>3. воздействия внешних факторов на систему</li> <li>4. преобразования в системе.</li> </ol> <p>- <b>Дайте определение понятия «информация».</b></p> <p>- <b>Дайте определение понятия «информатизация».</b></p>	
--	---	--



	<ul style="list-style-type: none"> <li>- <b>Дайте определение понятия «защита информации».</b></li> <li>- <b>Дайте определение понятия «целостность информации».</b></li> <li>- <b>Приведите примеры непреднамеренных угроз ИБ.</b></li> <li>- <b>Приведите примеры косвенных каналов утечки информации.</b></li> <li>- <b>Дайте определение понятию «информационная система».</b></li> <li>- <b>Какие бывают формы представления информации?</b></li> <li>- <b>Дайте определение понятию «утечка информации».</b></li> <li>- <b>Дайте определение понятию «конфиденциальность информации».</b></li> <li>- <b>Приведите примеры преднамеренных угроз ИБ.</b></li> <li>- <b>Приведите примеры непосредственных каналов утечки информации.</b></li> <li>- <b>Дайте определение персональных данных и назовите их категории.</b></li> <li>- <b>Дайте определение мониторинга информационной безопасности и назовите виды мониторинга.</b></li> </ul>	
--	---	--

### **Независимая оценка качества обучения**

Независимая оценка качества обучения предполагает внутренний аудит программ ДПО и анкетирование слушателей и/или работодателей по вопросам удовлетворенности процессом и результатами обучения.

### **Учебно-методическое и информационное обеспечение**

а) литература НТБ МЭИ:

1. Бабаш, А. В. Информационная безопасность: лабораторный практикум : учебное пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников . – 2-е изд., стереотип . – М. : КноРус, 2013 . – 136 с. + CD . – (Бакалавриат) . - ISBN 978-5-406-02760-8 .;

2. Информационная безопасность открытых систем. В 2 т. Т.1. Угрозы, уязвимости, атаки и подходы к защите : учебник для вузов по специальности 075500(090105) "Комплексное обеспечение информационной безопасности автоматизированных систем" / С. В. Запечников, и др. – М. : Горячая Линия-Телеком, 2006 . – 536 с. - ISBN 5-935172-91-1 .;

3. Информационная безопасность открытых систем. В 2 т. Т.2. Средства защиты в сетях : учебник для вузов по специальности 075500(090105) "Комплексное

обеспечение информационной безопасности автоматизированных систем" / С. В. Запечников, и др. – М. : Горячая Линия-Телеком, 2008 . – 558 с. - ISBN 978-5-9912003-4-9 .;

4. Малюк, А. А. Информационная безопасность: концептуальные и методологические основы защиты информации : учебное пособие для вузов по специальности 075400 "Комплексная защита объектов информации" / А. А. Малюк . – М. : Горячая Линия-Телеком, 2004 . – 280 с. - ISBN 5-935171-97-X .;

5. Партыка, Т. Л. Информационная безопасность : учебное пособие для среднего профессионального образования по специальностям информатики и вычислительной техники / Т. Л. Партыка, И. И. Попов . – 5-е изд., перераб. и доп . – М. : Форум : ИНФРА-М, 2014 . – 432 с. – (Профессиональное образование) . - ISBN 978-5-91134-627-0 .;

6. Федеральный закон "Об информации, информационных технологиях и защите информации: вступил в силу с 9 авг. 2006 г. – Новосибирск : Сиб. унив. изд-во, 2006 . – 16 с. – (Кодексы и законы России) . - ISBN 5-940877-41-9 .;

7. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие для среднего профессионального образования по группе специальностей "Информатика и вычислительная техника" / В. Ф. Шаньгин . – М. : Форум : ИНФРА-М, 2012 . – 416 с. – (Профессиональное образование) . - ISBN 978-5-8199-0331-5 .;

8. Ярочкин, В. И. Информационная безопасность : учебник для вузов по гуманитарным и социально-экономическим специальностям / В. И. Ярочкин ; Отв. ред. Л. И. Филиппенко . – 5-е изд . – М. : Академический проект, 2008 . – 544 с. – (Gaudeamus) . - ISBN 978-5-8291-0987-5 ..

б) литература ЭБС и БД:

*Не предусмотрено*

в) используемые ЭБС:

*Не предусмотрено*

Руководитель БИТ

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Кунбутаев Л.М.
	Идентификатор	R7a759843-KunbutayevLM-28fc24a

Л.М.  
Кунбутаев

Начальник ОДПО

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Крохин А.Г.
	Идентификатор	R6d4610d5-KrokhinAG-aa301f84

А.Г. Крохин