

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ  
ПО ДИСЦИПЛИНЕ**  
Основы информационной безопасности

**Код модуля**  
1163590(1)

**Модуль**  
Основы информационной безопасности

**Екатеринбург**

Оценочные материалы составлены автором(ами):

<b>№ п/п</b>	<b>Фамилия, имя, отчество</b>	<b>Ученая степень, ученое звание</b>	<b>Должность</b>	<b>Подразделение</b>
1	Лизовенко Ольга Александровна	без ученой степени, без ученого звания	Преподаватель	Учебно-научный центр "Информационная безопасность"
2	Поршнеv Сергей Владимирович	доктор технических наук, профессор	Профессор	Учебно-научный центр "Информационная безопасность"

**Согласовано:**

Управление образовательных программ

Т.Г. Комарова

**Авторы:**

- Лизовенко Ольга Александровна, Преподаватель, Учебно-научный центр "Информационная безопасность"
- Поршнев Сергей Владимирович, Профессор, Учебно-научный центр "Информационная безопасность"

## 1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Основы информационной безопасности

1.	Объем дисциплины в зачетных единицах	3	
2.	Виды аудиторных занятий	Лекции Практические/семинарские занятия	
3.	Промежуточная аттестация	Зачет	
4.	Текущая аттестация	Контрольная работа	1
		Домашняя работа	1

## 2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ Основы информационной безопасности

Индикатор – это признак / сигнал/ маркер, который показывает, на каком уровне обучающийся должен освоить результаты обучения и их предъявление должно подтвердить факт освоения предметного содержания данной дисциплины, указанного в табл. 1.3 РПМ-РПД.

Таблица 1

Код и наименование компетенции	Планируемые результаты обучения (индикаторы)	Контрольно-оценочные средства для оценивания достижения результата обучения по дисциплине
1	2	3
ПК-4 -Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской	3-1 - Различать правовые и организационные меры защиты информации, в том числе информации ограниченного доступа 3-2 - Изложить содержание нормативных правовых актов, нормативных и методических документов уполномоченных федеральных органов исполнительной власти (в том числе Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и	Домашняя работа Зачет Контрольная работа Лекции Практические/семинарские занятия

<p>Федерации, Федеральной службы по техническому и экспортному контролю</p>	<p>экспортному контролю) по защите информации П-1 - Осуществлять обоснованный выбор нормативной базы в области защиты информации ограниченного доступа У-1 - Формулировать организационно- распорядительные документы, регламентирующие защиту информации ограниченного доступа в автоматизированных системах</p>	
<p>ПК-8 -Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты</p>	<p>З-1 - Идентифицировать классификацию систем основные законы и закономерности систем информационной безопасности П-1 - Разрабатывать методики системного анализа У-1 - Выделять систему из внешней среды информационной безопасности</p>	<p>Домашняя работа Зачет Контрольная работа Лекции Практические/семинарские занятия</p>
<p>ПК-10 -Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма</p>	<p>З-1 - Описать основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в современном мире П-1 - Иметь практический опыт выбора принципов историзма и научной объективности как основой формирования собственной гражданской позиции и развития патриотизма У-1 - Формулировать и аргументировано отстаивать собственную позицию по различным проблемам истории России</p>	<p>Домашняя работа Зачет Контрольная работа Лекции Практические/семинарские занятия</p>

**3. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ МОДУЛЯ В БАЛЬНО-РЕЙТИНГОВОЙ СИСТЕМЕ (ТЕХНОЛОГИЧЕСКАЯ КАРТА БРС)**

**3.1. Процедуры текущей и промежуточной аттестации по дисциплине**

<b>1. Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0.5</b>		
Текущая аттестация на лекциях	Сроки – семестр, учебная неделя	Максимальная оценка в баллах
<i>контрольная работа</i>	2,7	100
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0.5		
Промежуточная аттестация по лекциям – <b>зачет</b>		
Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0.5		
<b>2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0.5</b>		
Текущая аттестация на практических/семинарских занятиях	Сроки – семестр, учебная неделя	Максимальная оценка в баллах
<i>домашняя работа</i>	2,14	100
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям – 1		
Промежуточная аттестация по практическим/семинарским занятиям – <b>нет</b>		
Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям – <b>не предусмотрено</b>		
<b>3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий – не предусмотрено</b>		
Текущая аттестация на лабораторных занятиях	Сроки – семестр, учебная неделя	Максимальная оценка в баллах
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям – <b>не предусмотрено</b>		
Промежуточная аттестация по лабораторным занятиям – <b>нет</b>		
Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям – <b>не предусмотрено</b>		
<b>4. Онлайн-занятия: коэффициент значимости совокупных результатов онлайн-занятий – не предусмотрено</b>		
Текущая аттестация на онлайн-занятиях	Сроки – семестр, учебная неделя	Максимальная оценка в баллах

<b>Весовой коэффициент значимости результатов текущей аттестации по онлайн-занятиям -не предусмотрено</b>
<b>Промежуточная аттестация по онлайн-занятиям –нет</b>
<b>Весовой коэффициент значимости результатов промежуточной аттестации по онлайн-занятиям – не предусмотрено</b>

### 3.2. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

<b>Текущая аттестация выполнения курсовой работы/проекта</b>	<b>Сроки – семестр, учебная неделя</b>	<b>Максимальная оценка в баллах</b>
<b>Весовой коэффициент текущей аттестации выполнения курсовой работы/проекта– не предусмотрено</b>		
<b>Весовой коэффициент промежуточной аттестации выполнения курсовой работы/проекта– защиты – не предусмотрено</b>		

## 4. КРИТЕРИИ И УРОВНИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ МОДУЛЯ

4.1. В рамках БРС применяются утвержденные на кафедре/институте критерии (признаки) оценивания достижений студентов по дисциплине модуля (табл. 4) в рамках контрольно-оценочных мероприятий на соответствие указанным в табл.1 результатам обучения (индикаторам).

Таблица 4

### Критерии оценивания учебных достижений обучающихся

<b>Результаты обучения</b>	<b>Критерии оценивания учебных достижений, обучающихся на соответствие результатам обучения/индикаторам</b>
Знания	Студент демонстрирует знания и понимание в области изучения на уровне указанных индикаторов и необходимые для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Умения	Студент может применять свои знания и понимание в контекстах, представленных в оценочных заданиях, демонстрирует освоение умений на уровне указанных индикаторов и необходимых для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Опыт /владение	Студент демонстрирует опыт в области изучения на уровне указанных индикаторов.
Другие результаты	Студент демонстрирует ответственность в освоении результатов обучения на уровне запланированных индикаторов. Студент способен выносить суждения, делать оценки и формулировать выводы в области изучения. Студент может сообщать преподавателю и коллегам своего уровня собственное понимание и умения в области изучения.

4.2 Для оценивания уровня выполнения критериев (уровня достижений обучающихся при проведении контрольно-оценочных мероприятий по дисциплине модуля) используется универсальная шкала (табл. 5).

Таблица 5

## Шкала оценивания достижения результатов обучения (индикаторов) по уровням

<b>Характеристика уровней достижения результатов обучения (индикаторов)</b>				
№ п/п	Содержание уровня выполнения критерия оценивания результатов обучения (выполненное оценочное задание)	Шкала оценивания		
		Традиционная характеристика уровня		Качественная характеристи ка уровня
1.	Результаты обучения (индикаторы) достигнуты в полном объеме, замечаний нет	Отлично (80-100 баллов)	Зачтено	Высокий (В)
2.	Результаты обучения (индикаторы) в целом достигнуты, имеются замечания, которые не требуют обязательного устранения	Хорошо (60-79 баллов)		Средний (С)
3.	Результаты обучения (индикаторы) достигнуты не в полной мере, есть замечания	Удовлетворительно (40-59 баллов)		Пороговый (П)
4.	Освоение результатов обучения не соответствует индикаторам, имеются существенные ошибки и замечания, требуется доработка	Неудовлетворитель но (менее 40 баллов)	Не зачтено	Недостаточный (Н)
5.	Результат обучения не достигнут, задание не выполнено	Недостаточно свидетельств для оценивания		Нет результата

### 5. СОДЕРЖАНИЕ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ПО ДИСЦИПЛИНЕ МОДУЛЯ

#### 5.1. Описание аудиторных контрольно-оценочных мероприятий по дисциплине модуля

##### 5.1.1. Лекции

Самостоятельное изучение теоретического материала по темам/разделам лекций в соответствии с содержанием дисциплины (п. 1.2. РПД)

##### 5.1.2. Практические/семинарские занятия

Примерный перечень тем

1. Информация как объект защиты
2. Анализ угроз информационной безопасности
3. Методы и средства обеспечения информационной безопасности
4. Модели, стратегии и системы обеспечения информационной безопасности
5. Международные стандарты информационной безопасности
6. Государственная политика в области информационной безопасности
7. Информационная война, методы и средства её ведения

Примерные задания

Необходимо провести анализ защищенности объекта защиты информации по следующим разделам:

1. Виды возможных угроз
2. Характер происхождения угроз
3. Классы каналов несанкционированного получения информации
4. Источники появления угроз
5. Причины нарушения целостности информации
6. Потенциально возможные злоумышленные действия
7. Определить класс защищенности автоматизированной системы  
LMS-платформа – не предусмотрена

## **5.2. Описание внеаудиторных контрольно-оценочных мероприятий и средств текущего контроля по дисциплине модуля**

Разноуровневое (дифференцированное) обучение.

### **Базовый**

#### **5.2.1. Контрольная работа**

Примерный перечень тем

1. Современные методы и средства обеспечения информационной безопасности

Примерные задания

1. ... - состояние защищенности информационных ресурсов от внутренних и внешних угроз, способных нанести ущерб интересам личности, общества, государства.

- 1) информационная безопасность
- 2) защита информации
- 3) национальная безопасность
- 4) обороноспособность

2. Семантический уровень представления информации связан с ...

- 1) смыслом записанной информации
- 2) используемым видом кодирования информации
- 3) используемой логикой записи информации на носитель
- 4) информацией, записанной на вещественных носителях

3. Угроза нарушения конфиденциальности реализуется в том случае, если информация становится известной ...

- 1) лицу, не располагающему полномочиями доступа к ней
- 2) любому лицу за пределами охраняемой зоны
- 3) средствам массовой информации
- 4) вероятному противнику

4. Меры защиты от НСД, регламентируемые внутренними инструкциями организации, эксплуатирующей информационную систему, относятся к ...

- 1) организационным
- 2) правовым



- 3) финансовым
- 4) инженерно-техническим
- 5) морально-этическим

5. Использование электронной подписи обеспечивает защиту ... информации

- (!) целостности
- (!) авторства
- (?) конфиденциальности
- (?) доступности

6. Модель разграничения доступа ... уязвима к вредоносным (троянским) программам, изменяющим направление потоков информации

- 1) Харрисона-Руззо-Ульмана
- 2) на основе паролей
- 3) Ла Падулы
- 4) Хартсона

7. Впервые понятие «профиль защиты» введено в ...

- 1) «Федеральных критериях безопасности информационных технологий»
- 2) «Критериях безопасности компьютерных систем»
- 3) «Европейских критериях безопасности информационных технологий»

8. ... создается для рассмотрения вопросов внутренней и внешней политики РФ в области обеспечения безопасности, стабильности и правопорядка

- 1) Совет безопасности РФ
- 2) Совет Федерации
- 3) ФСТЭК
- 4) МВД

LMS-платформа – не предусмотрена

### **5.2.2. Домашняя работа**

Примерный перечень тем

1. Информация как объект права собственности
2. Научно-технический прогресс и этапы развития защиты информации
3. Виды и формы представления информации
4. Обеспечение безопасности носителей информации
5. Защита информации в системах проводной связи
6. Защита информации в системах мобильной связи
7. Защита документальной информации
8. Защита личности как носителя информации
9. Методы и средства защиты информации от случайных воздействий
10. Физическая защита средств обработки и хранения информации
11. Электронно-цифровая подпись
12. Меры защиты информации, связанные с криптографией
13. Методы защиты от несанкционированного доступа к информации

14. Обеспечение безопасности персональных данных
15. Технология защиты распределённой системы
16. Современные средства антивирусной защиты
17. Обеспечение информационной безопасности в электронной торговле
18. Инженерные конструкции и сооружения для защиты информации
19. Оценка рисков информационной безопасности
20. Мировое сотрудничество в области информационной безопасности

#### Примерные задания

Домашняя работа выполняется в форме письменной работы (может быть выбрана форма реферативного изложения материала или эссе). Обязательным условием выполнения домашней работы является использование материалов статей актуальных периодических изданий. Работа должна содержать анализ обозначенной проблемы, требуется обоснование актуальности исследуемого вопроса. Ориентировочный объём исследовательского текста (включая цитирования) – 15-20 страниц. Домашняя работа выполняется студентами индивидуально и является обязательным контрольным мероприятием.

LMS-платформа – не предусмотрена

### **5.3. Описание контрольно-оценочных мероприятий промежуточного контроля по дисциплине модуля**

#### **5.3.1. Зачет**

Список примерных вопросов

1. Перечислите основные цели и задачи дисциплины «Основы информационной безопасности».
2. Какие методы защиты информации, использовавшиеся в древнее время и в средние века Вам известны?
3. Покажите связь между уровнем развития общества и технологиями защиты информации.
4. В каких направлениях идет развитие теории информационной безопасности в настоящее время?
5. Каков вклад российских ученых в теорию информационной безопасности?
6. С чем связан возросший интерес к проблемам защиты информации?
7. Каковы отличия формального и неформального подходов к проблемам защиты информации?
8. В чем, на Ваш взгляд, заключаются основные трудности обеспечения информационной безопасности в настоящее время?
9. Что такое информационная система? Телекоммуникационная система?
10. Каковы правовые понятия в области защиты информации? Что такое защита информации?
11. Охарактеризуйте понятия, связанные с организацией защиты информации. Каковы основные принципы построения систем защиты информации? Что такое информация и каковы уровни ее представления?
12. Перечислите основные носители информации, особенности их использования и защиты?

13. Какими свойствами определяется ценность информации? Какие критерии оценки ценности информации Вы можете предложить? Приведите примеры различной зависимости ценности информации от времени.
14. Что понимается под информационными ресурсами? Что не разрешается относить к информации ограниченного доступа?
15. Что понимается под конфиденциальной информацией? Какие существуют виды тайны?
16. Какое назначение имеет перечень конфиденциальных сведений предприятия?
17. Чем отличаются понятия «информационная война» и «информационное противоборство»? Чем отличается информационная война от «обычного» вооруженного конфликта?
18. Какие виды информационных войн Вы можете выделить? Приведите пример межкорпоративной информационной войны.
19. Можно ли рассматривать рекламу как средство ведения информационной борьбы?
20. Какие приемы ведения информационной войны используются во время предвыборных кампаний, приведите примеры.
21. Что такое информационное оружие? Какие виды оружия применяются в ходе ведения информационной войны? Каковы цели информационной войны?
22. Каковы средства и методы защиты от информационно-технического оружия? Каковы особенности информационно-психологической войны?
23. На примере нескольких различных угроз покажите, что их осуществление приведет к изменению одного из основных свойств защищаемой информации (конфиденциальности, целостности, доступности)
24. Приведите примеры систем, для которых наибольшую угрозу безопасности представляет нарушение конфиденциальности информации.
25. Для каких систем (приведите примеры) наибольшую опасность представляет нарушение целостности информации?
26. В каких системах на первом месте стоит обеспечение доступности информации?
27. В чем различие понятий «нарушение конфиденциальности информации», «несанкционированный доступ к информации», «утечка информации»?
28. Определите перечень основных угроз для АС, состоящей из автономно работающего компьютера без выхода в сеть, расположенной в одной из лабораторий университета.
29. Постройте неформальную модель нарушителя для учебной компьютерной лаборатории.
30. Выведите формулу для расчета прочности трехуровневой защитной оболочки.  
LMS-платформа – не предусмотрена

#### 5.4 Содержание контрольно-оценочных мероприятий по направлениям воспитательной деятельности

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения	Контрольно-оценочные мероприятия
Профессиональное воспитание	профориентационная	Технология формирования	ПК-4	П-1	Домашняя работа Зачет

	деятельность	уверенности и готовности к самостоятельной успешной профессиональной деятельности			Контрольная работа Практические/семинарские занятия
--	--------------	---	--	--	--