


АНО ВО «Межрегиональный открытый социальный институт»

УТВЕРЖДАЮ  
Зав. кафедрой информационной  
безопасности  
 Т.М. Гусакова  
Протокол заседания кафедры  
№ 01 «01» 09 2017г.

**Фонд оценочных средств  
для проведения текущего контроля успеваемости и промежуточной аттестации**

Учебная дисциплина «Основы информационной безопасности»

Образовательная программа  
10.03.01 Информационная безопасность.  
Комплексная защита объектов информатизации

Йошкар-Ола  
2017

## СОДЕРЖАНИЕ

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.
2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания.
3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы. – оценочные средства для текущего контроля; – оценочные средства для промежуточной аттестации.
4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

### 1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

В процессе освоения образовательной программы обучающиеся осваивают компетенции указанные в федеральных государственных образовательных стандартах высшего образования, сопоставленные с видами деятельности. Освоение компетенций происходит поэтапно через последовательное изучение учебных дисциплин, практик, подготовки ВКР и других видов работ предусмотренных учебным планом АНО ВО МОСИ.

№ п/п	Код компетенции	Формулировка компетенции	Номер этапа
1	ОПК-1	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	5/6
2	ПК-9	организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия	2/2

## 2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Этапами формирования компетенций обучающихся при освоении дисциплины являются последовательное изучение содержательно связанных между собой разделов (тем) учебных занятий. Результаты текущего контроля и промежуточной аттестации позволяют определить уровень освоения компетенций обучающимися.

### Перечень оценочных средств

№ п/п	Коды компетенций и планируемые результаты обучения		Оценочные средства	
			Наименование	Представление в ФОС
1	ОПК-1	<p><b>Знать:</b> об использовании основных положений теории информационной безопасности на различных уровнях (законодательном, административном, организационном, программно-техническом).</p> <p><b>Уметь:</b> правильно выбирать и применять меры законодательного, административного, организационного и программно-технического уровня для обеспечения информационной безопасности.</p> <p><b>Владеть:</b> внедрения и эксплуатации сервисов информационной безопасности программно-технического уровня, меры законодательного, административного и организационного уровней информационной безопасности.</p>	Устный опрос Практические задачи Реферат	Вопросы для устного опроса Практические задачи Темы рефератов

2	ПК-9	<p>Знать: о современных направлениях и перспективах развития защиты информации.</p> <p>Уметь: правильно проводить анализ угроз информационной безопасности, выполнять основные этапы решения задач информационной безопасности, применять на практике основные общеметодологические принципы теории информационной безопасности.</p> <p>Владеть: методами обеспечения информационной безопасности.</p>	<p>Устный опрос Практические задачи Реферат</p>	<p>Вопросы для устного опроса Практические задачи Темы рефератов</p>
---	------	--	---	--

### 3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

#### Текущая аттестация по дисциплине «Основы информационной безопасности»

Студенты ОП 38.03.05 Бизнес-информатика. Электронный бизнес проходят текущую аттестацию в 6/6-ом семестре.

Оценочные средства текущего контроля:

- *устный опрос,*
- *реферат,*
- *практические задачи*

#### Основные виды оценочных средств по темам представлены в таблице

№ п\п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1.	Тема 1 Понятие информационной безопасности, ее роль в национальной безопасности	ОПК-1, ПК-9	устный опрос, реферат, практические задачи
2.	Тема 2 Терминологические основы информационной безопасности	ОПК-1, ПК-9	устный опрос, доклад, реферат, практические задачи
3.	Тема 3 Угрозы. Классификация и анализ угроз информационной безопасности	ОПК-1, ПК-9	устный опрос, практические задачи, реферат
4.	Тема 4 Модель угроз, модель нарушителя	ОПК-1, ПК-9	устный опрос, реферат, практические задачи
5.	Тема 5 Модели оценки угроз конфиденциальности, целостности, доступности	ОПК-1, ПК-9	устный опрос, реферат, практические задачи
6.	Тема 6 Функции и задачи защиты информации	ОПК-1, ПК-9	устный опрос, реферат, практические задачи
7.	Тема 7 Проблемы региональной информационной безопасности	ОПК-1, ПК-9	устный опрос, реферат, практические задачи

#### Вопросы для устного опроса

1. Назовите органы, обеспечивающие национальную безопасность Российской Федерации, цели, задачи.
2. Охарактеризуйте национальные интересы Российской Федерации в информационной сфере. Каковы приоритетные направления в области защиты информации в Российской Федерации?
3. Каковы тенденции развития информационной политики государств и ведомств? Что такое информационная война?
4. Охарактеризуйте правовое обеспечение защиты информации.
5. Что такое информация с ограниченным доступом, государственная тайна, конфиденциальность, коммерческая тайна, персональные данные?
6. Что такое информация? Дайте характеристику смежным с ним понятиям: информационная безопасность, информационная война, информационная агрессия,

информационное оружие, информационные процессы, информационная система, информационная сфера, виды информации.

7. Кто такое автор и собственник информации? Как взаимодействуют субъекты в информационном обмене?

8. Что такое защита информации, тайна, средства защиты информации, угрозы?

9. Что такое идентификация, аутентификация, авторизация?

10. Что такое угроза? Перечислите виды угроз.

11. Охарактеризуйте три наиболее выраженные угрозы: 1) подверженность физическому искажению или уничтожению; 2) возможность несанкционированной (случайной или злоумышленной) модификации; 3) опасность несанкционированного (случайного и преднамеренного) получения информации лицами, для которых она не предназначена.

12. Назовите особенности происхождения угроз: умышленные факторы, естественные факторы.

13. Каковы источники угроз?

14. Назовите предпосылки появления угроз: объективные, субъективные.

15. Дайте характеристику классам каналов несанкционированного получения информации: 1) непосредственно с объекта; 2) с каналов отображения информации; 3) получение по внешним каналам; 4) подключение к каналам получения информации.

16. Назовите причины нарушения целостности информации: субъективные преднамеренные, субъективные непреднамеренные, объективные непреднамеренные.

17. Назовите потенциально возможные злоумышленные действия в автоматизированных системах обработки данных.

18. Как происходит формирование модели нарушителя?

19. Назовите три методологических подхода к оценке уязвимости информации: эмпирический, теоретический и теоретико-эмпирический.

20. Какова модель затрат, разработанная специалистами американской фирмы IBM. Модель защиты — модель системы с полным перекрытием.

21. Какова последовательность решения задачи защиты информации?

22. Назовите фундаментальные требования, которым должны удовлетворять те вычислительные системы, которые используются для обработки конфиденциальной информации.

23. Дайте классификацию автоматизированных систем и требований по защите информации. Назовите факторы, влияющие на требуемый уровень защиты информации.

24. Перечислите методы формирования функций защиты. Как происходит скрытие информации о средствах, комплексах, объектах и системах обработки информации?

25. Что такое дезинформация противника? Что такое легендирование? Как происходит резервирование элементов системы?

26. Как происходит регулирование доступа к элементам системы и защищаемой информации. Как происходит регулирование использования элементов системы и защищаемой информации?

27. Что такое маскировка информации? Как происходит регистрация сведений? Как уничтожается информация? Обеспечение сигнализации. Обеспечение реагирования.

28. Что такое управление системой защиты информации? Как происходит обеспечение требуемого уровня готовности обслуживающего персонала к решению задач информационной безопасности.

29. Как осуществляется защита от информационного воздействия на технические средства обработки? Что такое защита от информационного воздействия на общество? Как осуществляется защита от информационного воздействия на психику человека?

30. Что такое региональные компоненты защиты информации?

31. Как осуществляется защита информации предприятия?

32. Как проводится анализ защищенности локального объекта?

## **Средство оценивания: устный опрос**

Шкала оценивания:

– оценка «отлично» выставляется студенту, если студент не только глубоко и прочно усвоил весь программный материал, но и проявил знания, выходящие за его пределы, почерпнутые из дополнительных источников (учебная литература, научно-популярная литература, научные статьи и монографии, сборники научных трудов и интернет-ресурсы и т. п.); умеет самостоятельно обобщать программный материал, не допуская ошибок, проанализировать его с точки зрения различных школ и взглядов; увязывает знания с практикой; приводит примеры, демонстрирующие глубокое понимание материала или проблемы;

– оценка «хорошо» выставляется студенту, если студент твердо знает программный материал, грамотно и последовательно его излагает, увязывает с практикой, не допуская существенных неточностей в ответе на вопросы;

– оценка «удовлетворительно» выставляется студенту, если студент усвоил только основной программный материал, но не знает отдельных положений, в ответе допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении программного материала;

– оценка «неудовлетворительно» выставляется студенту, если студент не знает значительной части основного программного материала, в ответе допускает существенные ошибки, неправильные формулировки.

### **Перечень тем рефератов по дисциплине «Основы информационной безопасности»**

1. Методы борьбы с фишинговыми атаками.
2. Законодательство о персональных данных.
3. Защита авторских прав.
4. Назначение, функции и типы систем видеозащиты.
5. Как подписывать с помощью ЭЦП электронные документы различных форматов.
6. Обзор угроз и технологий защиты Wi-Fi-сетей.
7. Проблемы внедрения дискового шифрования.
8. Борьба со спамом: основные подходы, классификация, примеры, прогнозы на будущее.
9. Особенности процессов аутентификации в корпоративной среде.
10. Квантовая криптография.
11. Утечки информации: как избежать. Безопасность смартфонов.
12. Безопасность применения пластиковых карт - законодательство и практика.
13. Защита CD- и DVD-дисков от копирования.
14. Современные угрозы и защита электронной почты.
15. Программные средства анализа локальных сетей на предмет уязвимостей.
16. Безопасность применения платежных систем - законодательство и практика.
17. Аудит программного кода по требованиям безопасности.
18. Антишпионское ПО (antispysware).
19. Обеспечение безопасности Web-сервисов.
20. Защита от внутренних угроз.
21. Технологии RFID.
22. Уничтожение информации на магнитных носителях.
23. Ботнеты - плацдарм современных кибератак.
24. Цифровые водяные знаки в изображениях.
25. Электронный документооборот. Модели нарушителя.
26. Идентификация по голосу. Скрытые возможности.
27. Безопасность океанских портов.
28. Безопасность связи.
29. Безопасность розничной торговли.



30. Банковская безопасность.
31. Информатизация управления транспортной безопасностью.
32. Биопаспорт.
33. Обзор современных платформ архивации данных.
34. Что такое консалтинг в области ИБ.
35. Бухгалтерская отчетность как источник рассекречивания информации.
36. Управление рисками: обзор потребительских подходов.
37. Категорирование информации и информационных систем. Обеспечение базового уровня информационной безопасности.
38. Распределенные атаки на распределенные системы.
39. Оценка безопасности автоматизированных систем.
40. Windows и Linux: что безопаснее?
41. Функциональная безопасность программных средств.
42. Технологические процессы и стандарты обеспечения функциональной безопасности в жизненном цикле программных средств.
43. Информационная безопасность: экономические аспекты.

### Средство оценивания: реферат

Шкала оценивания:

Реферат оценивается по 100-балльной шкале. Баллы переводятся в оценки успеваемости следующим образом:

- 86-100 баллов – «отлично»;
- 70- 85 баллов – «хорошо»;
- 51-69 баллов – «удовлетворительно»;
- менее 51 балла – «неудовлетворительно».

Критерии	Показатели
1. Новизна реферированного текста. Максимальная оценка – 20 баллов	актуальность проблемы и темы; – новизна и самостоятельность в постановке проблемы, в формулировании нового аспекта выбранной для анализа проблемы; – наличие авторской позиции, самостоятельность суждений.
2. Степень раскрытия сущности проблемы. Максимальная оценка – 30 баллов	– соответствие плана теме реферата; – соответствие содержания теме и плану реферата; – полнота и глубина раскрытия основных понятий проблемы; – обоснованность способов и методов работы с материалом; – умение работать с историческими источниками и литературой, систематизировать и структурировать материал; – умение обобщать, сопоставлять различные точки зрения по рассматриваемому вопросу, аргументировать основные положения и выводы
3. Обоснованность выбора источников и литературы. Максимальная оценка – 20	круг, полнота использования исторических источников и литературы по проблеме;

баллов	– привлечение новейших работ по проблеме (журнальные публикации, материалы сборников научных трудов, интернет-ресурсов и т. д.).
4. Соблюдение требований к оформлению. Максимальная оценка – 15 баллов.	<p>правильное оформление ссылок на использованные источники и литературу;</p> <p>– грамотность и культура изложения;</p> <p>– использование рекомендованного количества исторических источников и литературы;</p> <p>– владение терминологией и понятийным аппаратом проблемы;</p> <p>– соблюдение требований к объему реферата;</p> <p>– культура оформления: выделение абзацев, глав и параграфов</p>
5. Грамотность. Максимальная оценка – 15 баллов.	<p>– отсутствие орфографических и синтаксических ошибок, стилистических погрешностей;</p> <p>– отсутствие опечаток, сокращений слов, кроме общепринятых;</p> <p>– литературный стиль.</p>

## **Перечень практических заданий**

### **Задание 1. Методы поиска и сбора информации.**

Цель работы: Приобретение навыков поиска информации используя поисковые системы.

Задачи:

1. Поисковые системы. Методика поиска.
2. Рассылки, тематические форумы.
3. Возможности использования иноязычных ресурсов.

### **Задание 2. Методика устранения компьютерной информации.**

Цель работы: Приобретение навыков устранения и восстановления информации на различных носителях.

Задачи:

1. Физическая организация жестких дисков.
2. Методы восстановления информации.
3. Обзор современных средств устранения компьютерной информации.

### **Задание 3. Уязвимости Windows.**

Цель работы: Приобретение навыков настройки Windows для уменьшения уязвимостей.

Задачи:

1. Недостатки архитектуры операционных систем семейства Windows .
2. Основные виды уязвимостей: статистика их обнаружения и устранения.
3. Описание методик атак, использующих уязвимости операционной системы семейства Windows.
4. Настройка операционной системы для увеличения обороноспособности вычислительной системы.

### **Задание 4. Защита от копирования переносных носителей.**

Цель работы: Приобретение навыков защиты от копирования переносных носителей.

Задачи:

1. Методика защиты программных и установочных дисков.
2. Методика защиты дисков с данными.
3. Современные средства защиты видеодисков.

### **Задание 4. Аппаратные ключи защиты.**

Цель работы: Приобретение навыков защиты данных с помощью аппаратных ключей.

Задачи:

1. Основные виды аппаратных ключей.
2. Методики обхода аппаратных ключей.
3. Недостатки аппаратных ключей

### **Задание 5. Навесная защита**

Цель работы: Приобретение навыков защиты информации используя программное обеспечение.

Задачи:

1. Методика установки протекторов.
2. Работа протекторов.
3. Недостатки протекторов.

### **Задание 6. Антивирусное программное обеспечение.**

Цель работы: Приобретение навыков защиты информации используя антивирусное программное обеспечение.

Задачи:

1. Программы-шпионы. Защита от программ шпионов.
2. Троянские программы.

3. "Черви", методики проникновения.
4. Вирусы, алгоритмы работы.
5. Антивирусное программное обеспечение: рекомендуемые настройки, правила использования.

**Задание 7. Особенности защиты информации при работе в сети.**

Цель работы: Приобретение навыков защиты информации при работе в сети.

Задачи:

1. Средства управления сетями.
2. Программные средства обеспечения защиты информации в локальной сети.
3. Обязанности администратора сети, относящиеся к безопасности информации.
4. Средства обнаружения сетевых атак.

**Задание 8. Безопасная работа в Internet.**

Цель работы: Приобретение навыков безопасной работы в сети интернет.

Задачи:

1. Выбор сайтов для посещения.
2. Настройка встроенных средств защиты информации современных браузеров.
3. Обработка сообщений электронной почты. Спам-фильтры.
4. Ограничение доступа из локальной сети в Internet с помощью прокси- серверов.
5. Типы межсетевых экранов, их достоинства и недостатки

**Средство оценивания: Практические задания**

Шкала оценивания:

Практическое задание оценивается по 5-балльной шкале. Баллы переводятся в оценки успеваемости следующим образом:

Оценка «отлично» выставляется обучающемуся, если практическое задание правильно решено, приведена подробная аргументация своего решение, показано хорошее знание теоретических аспектов ее решения.

Оценка «хорошо» выставляется обучающемуся, если практическое задание правильно решено, приведена достаточная аргументация своего решение, показано определенное знание теоретических материала.

Оценка «удовлетворительно» выставляется обучающемуся, если практическое задание частично имеет правильное решение, аргументация не полная, не прослеживается знание теоретических материала.

Оценка «неудовлетворительно» выставляется обучающемуся, если практическое задание решено неверно, отсутствуют необходимые знания теоретического материала.

## Промежуточная аттестация по дисциплине «Основы информационной безопасности»

Студенты ОП 38.03.05 Бизнес-информатика. Электронный бизнес проходят промежуточную аттестацию в форме зачета по дисциплине "Основы информационной безопасности" в 6/6 семестре.

При проведении зачета по дисциплине «Основы информационной безопасности» может использоваться устная или письменная форма проведения.

### Примерная структура зачета по дисциплине «Основы информационной безопасности»

#### 1. устный ответ на вопросы

Студенту на зачете дается время на подготовку вопросов теоретического характера

#### 2. выполнение тестовых заданий

Тестовые задания выполняются в течение 30 минут и состоят из 25 вопросов разных типов. Преподаватель готовит несколько вариантов тестовых заданий.

#### 3. выполнение практических заданий

Практических задания выполняются в течение 30 минут. Бланки с задачами готовит и выдает преподаватель.

#### Устный ответ студента на зачете должен отвечать следующим требованиям:

- научность, знание и умение пользоваться понятийным аппаратом;
- изложение вопросов в методологическом аспектах, аргументация основных положений ответа примерами из современной практики, а также из личного опыта работы;
- осведомленность в важнейших современных проблемах информационной безопасности, знание классической и современной литературы.

#### Выполнение практического задания должно отвечать следующим требованиям:

- Владение профессиональной терминологией;
- Последовательное и аргументированное изложение решения.

### Критерии оценивания ответов

	Устный ответ	Практическое задание	Тестовые задания
<i>зачтено</i>	знание учебного материала в пределах программы; логическое, последовательное изложение вопроса; определение своей позиции в раскрытии различных подходов к рассматриваемой проблеме;	свободное владение профессиональной терминологией; умение высказывать и обосновать свои суждения; студент дает четкий, полный анализ ситуации.	50-100 % правильно выполненных заданий
<i>не зачтено</i>	пробелы в знаниях основного учебно-программного материала, принципиальные ошибки в изложении материала	допущены ошибки в определении понятий, искажен их смысл; студент не может применять знания для решения практического задания.	До 50 % правильно выполненных заданий

### Критерии и шкала оценивания уровней освоения компетенций

Шкала оценивания	Шкала оценивания	Шкала оценивания
отлично	высокий	студент, овладел элементами компетенции «знать», «уметь» и «владеть», проявил всесторонние и

		глубокие знания программного материала по дисциплине, освоил основную и дополнительную литературу, обнаружил творческие способности в понимании, изложении и практическом использовании усвоенных знаний.
хорошо	продвинутый	студент овладел элементами компетенции «знать» и «уметь», проявил полное знание программного материала по дисциплине, освоил основную рекомендованную литературу, обнаружил стабильный характер знаний и умений и проявил способности к их самостоятельному применению и обновлению в ходе последующего обучения и практической деятельности.
удовлетворительно	базовый	студент овладел элементами компетенции «знать», проявил знания основного программного материала по дисциплине в объеме, необходимом для последующего обучения и предстоящей практической деятельности, изучил основную рекомендованную литературу, допустил неточности в ответе на экзамене, но в основном обладает необходимыми знаниями для их устранения при корректировке со стороны экзаменатора.
неудовлетворительно	компетенции не сформированы	студент не овладел ни одним из элементов компетенции, обнаружил существенные пробелы в знании основного программного материала по дисциплине, допустил принципиальные ошибки при применении теоретических знаний, которые не позволяют ему продолжить обучение или приступить к практической деятельности без дополнительной подготовки по данной дисциплине.

Оценка «зачтено» соответствует критериям оценок от «отлично» до «удовлетворительно».

Оценка «не зачтено» соответствует критерию оценки «неудовлетворительно»

**Отметка** за зачет по предмету выставляется с учетом полученных отметок в соответствии с правилами математического округления.

#### **Рекомендации по проведению зачета**

1. Студенты должны быть заранее ознакомлены с требованиями к зачету, критериями оценивания.

2. Необходимо выяснить на зачете, формально или нет владеет студент знаниями по данному предмету. Вопросы при ответе по билету помогут выяснить степень понимания студентом материала, знание им связей излагаемого вопроса с другими изучавшимися им понятиями, а практические задания – умения применять знания на практике.

3. На зачете следует выяснить, как студент знает программный материал, как он им овладел к моменту зачета, как он продумал его в процессе обучения и подготовки к зачету.

4. При устном опросе целесообразно начинать с легких, простых вопросов, ответы на которые помогут подготовить студента к спокойному размышлению над дальнейшими более трудными вопросами и практическими заданиями.

5. Тестирование по дисциплине проводится либо в компьютерном классе, либо в аудитории на бланке с тестовыми заданиями.

Во время тестирования обучающиеся могут пользоваться калькулятором. Результат каждого обучающегося оценивается в соответствии с оценочной шкалой, приведённой в пункте 3.

6. Выполнение практических заданий осуществляется в учебной аудитории. Результат каждого обучающегося оценивается в соответствии с оценочной шкалой, приведённой в пункте 3.

#### **Перечень вопросов к зачету**

1. Теория защиты информации. Основные направления
2. Обеспечение информационной безопасности и направления защиты
3. Комплексность (целевая, инструментальная, структурная, функциональная, временная)
4. Требования к системе защиты информации
5. Угрозы информации
6. Виды угроз. Основные нарушения
7. Характер происхождения угроз
8. Источники угроз. Предпосылки появления угроз
9. Система защиты информации
10. Классы каналов несанкционированного получения информации
11. Причины нарушения целостности информации
12. Методы и модели оценки уязвимости информации
13. Общая модель воздействия на информацию
14. Общая модель процесса нарушения физической целостности информации
15. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных
16. Методологические подходы к оценке уязвимости информации
17. Модель защиты системы с полным перекрытием
18. Рекомендации по использованию моделей оценки уязвимости информации
19. Допущения в моделях оценки уязвимости информации
20. Методы определения требований к защите информации
21. Факторы, обуславливающие конкретные требования к защите, обусловленные спецификой автоматизированной обработки информации
22. Классификация требований к средствам защиты информации
23. Требования к защите, определяемые структурой автоматизированной системы обработки данных
24. Требования к защите, обуславливаемые видом защищаемой информации
25. Требования, обуславливаемые, взаимодействием пользователя с комплексом средств автоматизации
26. Анализ существующих методик определения требований к защите информации
27. Стандарт США "Критерии оценки гарантировано защищенных вычислительных систем в интересах министерства обороны США". Основные положения
28. Руководящий документ Гостехкомиссии России "Классификация автоматизированных систем и требований по защите информации", выпущенном в 1992 году. Часть 1
29. Классы защищенности средств вычислительной техники от несанкционированного доступа – Функции защиты информации
30. Стратегии защиты информации
31. Способы и средства защиты информации
32. Способы "абсолютной системы защиты"
33. Архитектура систем защиты информации. Требования
34. Общеметодологических принципов архитектуры системы защиты информации
35. Построение средств защиты информации

- 36. Ядро системы защиты
- 37. Семирубевная модель защиты
- 38. Средства защиты информации. Антивирусы, средства анализа защищенности, средства обнаружения вторжений
- 39. Регуляторы в области защиты информации

### **Тест по дисциплине «Основы информационной безопасности»**

#### **0 вариант**

Как называется умышленно искаженная информация?

- + Дезинформация
- Информативный поток
- Достоверная информация
- Перестает быть информацией

Как называется информация, к которой ограничен доступ?

- + Конфиденциальная
- Противозаконная
- Открытая
- Недоступная

Какими путями может быть получена информация?

- + проведением, покупкой и противоправным добыванием информации научных исследований
- захватом и взломом ПК информации научных исследований
- добыванием информации из внешних источников и скремблированием информации научных исследований
- захватом и взломом защитной системы для информации научных исследований

Как называются компьютерные системы, в которых обеспечивается безопасность информации?

- + защищенные КС
- небезопасные КС
- Само достаточные КС
- Саморегулирующиеся КС

Основной документ, на основе которого проводится политика информационной безопасности?

- + программа информационной безопасности
- регламент информационной безопасности
- политическая информационная безопасность
- Протекторат

В зависимости от формы представления информация может быть разделена на?

- + Речевую, документированную и телекоммуникационную
- Мысль, слово и речь
- цифровая, звуковая и тайная
- цифровая, звуковая

К каким процессам относят процессы сбора, обработки, накопления, хранения, поиска и распространения информации

- + Информационным процессам
- Мыслительным процессам



- Машинным процессам
- Микропроцессам

Что называют защитой информации?

- + Все ответы верны
- Называют деятельность по предотвращению утечки защищаемой информации
- Называют деятельность по предотвращению несанкционированных воздействий на защищаемую информацию
- Называют деятельность по предотвращению непреднамеренных воздействий на защищаемую информацию

Под непреднамеренным воздействием на защищаемую информацию понимают?

- + Воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств и воздействие природных явлений
- Процесс ее преобразования, при котором содержание информации изменяется на ложную
- Возможности ее преобразования, при котором содержание информации изменяется на ложную информацию
- Не ограничения доступа в отдельные отрасли экономики или на конкретные производства

Шифрование информации - это

- + Процесс ее преобразования, при котором содержание информации становится непонятным для не обладающих соответствующими полномочиями субъектов
- Процесс преобразования, при котором информация удаляется
- Процесс ее преобразования, при котором содержание информации изменяется на ложную
- Процесс преобразования информации в машинный код

Основные предметные направления Защиты Информации?

- + охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности
- Охрана золотого фонда страны
- Определение ценности информации
- Усовершенствование скорости передачи информации

Государственная тайна – это

- + защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны
- ограничения доступа в отдельные отрасли экономики или на конкретные производства
- защищаемые банками и иными кредитными организациями сведения о банковских операциях
- защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

Коммерческая тайна - это...

- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны

+ ограничения доступа в отдельные отрасли экономики или на конкретные производства

- защищаемые банками и иными кредитными организациями сведения о банковских операциях

- защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

Банковская тайна - это...

- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны

- ограничения доступа в отдельные отрасли экономики или на конкретные производства

+ защищаемые банками и иными кредитными организациями сведения о банковских операциях

- защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

Профессиональная тайна

- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны

- ограничения доступа в отдельные отрасли экономики или на конкретные производства

- защищаемые банками и иными кредитными организациями сведения о банковских операциях

+ защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

К основным объектам банковской тайны относятся следующие:

+ Все ответы верны

- Тайна банковского счета

- Тайна операций по банковскому счету

- Тайна банковского вклада

Как называется тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений?

+ Тайна связи

- Нотариальная тайна

- Адвокатская тайна

- Тайна страхования

Как называются сведения, доверенные нотариусу в связи с совершением нотариальных действий?

+ Нотариальная тайна

- Общедоступные сведения

- Нотариальный секрет
- Нотариальное вето

Элемент аппаратной защиты, где используется установка источников бесперебойного питания (UPS)?

- + защита от сбоев в электропитании
- защита от сбоев серверов, рабочих станций и локальных компьютеров
- защита от сбоев устройств для хранения информации
- защита от утечек информации электромагнитных излучений

Функция защиты информационной системы, гарантирующая то, что доступ к информации, хранящейся в системе может быть осуществлен только тем лицам, которые на это имеют право

- управление доступом
- + конфиденциальность
- аутентичность
- целостность
- доступность

Элемент аппаратной защиты, где используется резервирование особо важных компьютерных подсистем

- защита от сбоев в электропитании
- + защита от сбоев серверов, рабочих станций и локальных компьютеров
- защита от сбоев устройств для хранения информации
- защита от утечек информации электромагнитных излучений

Элемент аппаратной защиты, где используется организация надежной и эффективной системы резервного копирования и дублирования данных

- защита от сбоев в электропитании
- защита от сбоев серверов, рабочих станций и локальных компьютеров
- + защита от сбоев устройств для хранения информации
- защита от утечек информации электромагнитных излучений

Элемент аппаратной защиты, где используется экранирование, фильтрацию, заземление, электромагнитное зашумление, а также средства ослабления уровней нежелательных электромагнитных излучений.

- защита от сбоев в электропитании
- защита от сбоев серверов, рабочих станций и локальных компьютеров
- защита от сбоев устройств для хранения информации
- + защита от утечек информации электромагнитных излучений

Какая из перечисленных атак на поток информации является пассивной:

- + перехват.
- имитация.
- модификация.
- фальсификация.
- прерывание.

К открытым источникам информация относится.

- + Газеты, Радио, Новости
- Информация украденная у спецслужб
- Из вскрытого сейфа

- Украденная из правительственной организации

Технические каналы утечки информации делятся на...

+ Все перечисленное

- Акустические и виброакустические

- Электрические

- Оптические

Какой технический канал утечки отвечает за распространение звуковых колебаний в любом звукопроводящем материале или среде?

+ Акустические и виброакустические

- Электрические

- Оптические

- Радиоканалы

Какой технический канал утечки отвечает за напряжение и токи в различных токопроводящих коммуникациях?

- Акустические и виброакустические

+ Электрические

- Оптические

- Радиоканалы

Какой технический канал утечки отвечает за электромагнитные излучения радиодиапазона?

- Акустические и виброакустические

- Электрические

- Оптические

+ Радиоканалы

Какой технический канал утечки отвечает за электромагнитные излучения в видимой, инфракрасной и ультрафиолетовой частях спектра?

- Акустические и виброакустические

- Электрические

+ Оптические

- Радиоканалы

## **Примерный перечень практических заданий**

### **Первое задание**

Для выполнения первой части необходимо для выбранного определенного объекта защиты информации необходимо описать объект защиты, провести анализ защищенности объекта защиты информации по следующим разделам:

1. виды угроз;
2. характер происхождения угроз;
3. классы каналов несанкционированного получения информации;
4. источники появления угроз;
5. причины нарушения целостности информации;
6. потенциально возможные злоумышленных действий;
7. определить класс защиты информации.

### **Второе задание**

Для выполнения второго задания предложить анализ увеличения защищенности объекта защиты информации по следующим разделам:

1. определить требования к защите информации;

2. классифицировать автоматизированную систему;
3. определить факторы, влияющие на требуемый уровень защиты информации;
4. выбрать или разработать способы и средства защиты информации;
5. построить архитектуру систем защиты информации;
6. сформулировать рекомендации по увеличению уровня защищенности.

**Наименование объекта защиты информации:**

1. Одиночно стоящий компьютер в бухгалтерии.
2. Сервер в бухгалтерии.
3. Почтовый сервер.
4. Веб-сервер.
5. Компьютерная сеть материальной группы.
6. Одноранговая локальная сеть без выхода в Интернет.
7. Одноранговая локальная сеть с выходом в Интернет.
8. Сеть с выделенным сервером без выхода в Интернет.
9. Сеть с выделенным сервером с выхода в Интернет.
10. Телефонная база данных (содержащая и информацию ограниченного пользования) в твердой копии и на электронных носителях.
11. Телефонная сеть.
12. Средства телекоммуникации (радиотелефоны, мобильные телефоны, пейджеры).
13. Банковские операции (внесение денег на счет и снятие).
14. Операции с банковскими пластиковыми карточками.
15. Компьютер, хранящий конфиденциальную информацию о сотрудниках предприятия.
16. Компьютер, хранящий конфиденциальную информацию о разработках предприятия.
17. Материалы для служебного пользования на твердых носителях в производстве.
18. Материалы для служебного пользования на твердых носителях на закрытом предприятии.
19. Материалы для служебного пользования на твердых носителях в архиве.
20. Материалы для служебного пользования на твердых носителях в налоговой инспекции.
21. Комната для переговоров по сделкам на охраняемой территории.
22. Комната для переговоров по сделкам на неохраняемой территории.
23. Сведения для средств массовой информации, цензура на различных носителях информации (твердая копия, фотографии, электронные носители и др.).
24. Судебные материалы (твердая копия).
25. Паспортный стол РОВД.
26. Материалы по владельцам автомобилей (твердая копия, фотографии, электронные носители и др.).
27. Материалы по недвижимости (твердая копия, фотографии, электронные носители и др.).
28. Сведения по тоталитарным сектам и другим общественно-вредным организациям.
29. Сведения по общественно-полезным организациям (красный крест и др.).
30. Партийные списки и руководящие документы.

#### **4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций**

Средство оценивания: реферат

##### **МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПОДГОТОВКЕ РЕФЕРАТА**

Тему реферата студент выбирает самостоятельно, ориентируясь на прилагаемый примерный список. В реферате студенты показывают знания дисциплины и умение реферировать, т. е. творчески анализировать прочитанный текст, а также умение аргументированно и ясно представлять свои мысли, с обязательными ссылками на использованные источники и литературу. В реферате желательно отразить различные точки зрения по вопросам выбранной темы.

Реферат следует писать в определенной последовательности. Студенту необходимо ознакомиться с Программой курса по истории, выбрать нужную тему, подобрать и изучить рекомендованные документы и литературу. Если заинтересовавшая студента тема не учтена в прилагаемом списке, то по согласованию с преподавателем можно предложить свою. Выбирая тему реферата, необходимо руководствоваться личным интересом и доступностью необходимых источников и литературы.

Поиск литературы по избранной теме следует осуществлять в систематическом и генеральном (алфавитном) каталогах библиотек (по фамилии автора или названию издания) на библиографических карточках или в электронном виде. Поиск литературы (особенно статей в сборниках и в коллективных монографиях) облегчит консультация с библиографом библиотеки. Возможен также поиск перечней литературы и источников по информационным сетевым ресурсам (Интернета).

Ознакомившись с литературой, студент отбирает для своего реферата несколько научных работ (монографий, статей и др.). Выбирая нужную литературу, следует обратить внимание на выходные данные работы.

Объем реферата колеблется в пределах 25-30 страниц формата А-4 с кеглем 14 и полуторным интервалом между строками в обычной компьютерной редакторской программе. Отредактированная работа должна быть пронумерована (номер ставится в верхней части страницы, по центру) и сброшюрована.

Реферат должен быть оформлен в компьютерном варианте. Компьютерный текст должен быть выполнен следующим образом:

- текст набирается на одной стороне листа;
- стандартная страница формата А4 имеет следующие поля: правое – 10 мм, левое – 30 мм, верхнее и нижнее – 20 мм;
- межстрочный интервал – полуторный;
- гарнитура шрифта – Times New Roman;
- кегль шрифта – 14;
- абзацный отступ – 1,25 пт.

На титульном листе, который не нумеруется, указывается название учебного заведения, кафедры, полное название темы реферата, курс, отделение, номер учебной группы, инициалы и фамилия студента, а также ученая степень, ученое звание, инициалы и фамилия преподавателя, который будет проверять работу.

На второй странице размещается оглавление реферата, которое отражает структуру реферата и включает следующие разделы:

– введение, в котором необходимо обосновать выбор темы, сформулировать цель и основные задачи своего исследования, а также можно отразить методику исследования;

– основная часть, состоящая из нескольких глав, которые выстраиваются по хронологическому или тематическому принципу, озаглавливаются в соответствии с

проблемами, рассматриваемыми в реферате. Главы желательно разбивать на параграфы. Важно, чтобы разделы оглавления были построены логично, последовательно и наилучшим образом раскрывали тему реферата;

– заключение, в котором следует подвести итоги изучения темы, на основании источников, литературы и собственного понимания проблемы изложить свои выводы.

Ссылки на источники и литературу, использованные в реферате, обозначаются цифрами в положении верхнего индекса, а в подстрочных сносках (внизу страницы) указывается источник, на который ссылается автор. Сноска должна быть полной: с указанием фамилии и инициалов автора, названия книги, места и года ее издания, страницы, на которую сделана ссылка в тексте.

Цитирование (буквальное воспроизведение) текста других авторов в реферате следует использовать лишь в тех случаях, когда необходимо привести принципиальные положения, оптимально сформулированные выводы и оценки, прямую речь, фрагмент документа и пр. В цитате недопустима любая замена слов. Если в работе содержатся выдержки (цитаты) из отдельных произведений или источников, их следует заключить в кавычки и указать источник, откуда взята данная цитата (автор, название сочинения, год и место издания, страница, например: Маршалова А. С. Система государственного и муниципального управления: Учебное пособие. – М., 2009. – С. 10.). Издательство в сносках обычно не указывается.

В реферате допускается передача того или иного эпизода или определенной мысли своими словами. В этом случае в тексте кавычки не ставятся, но в подстрочном примечании следует указать выходные данные источника. В тех случаях, когда сноска делается повторно на одно и то же издание, тогда в подстрочном примечании выходные данные не приводятся полностью.

Например:

Выработка политических ориентиров в значительной степени основана не на строго рациональном или научном анализе, а на понимании необходимости защиты тех или иных социальных интересов, осознании характера сопутствующей им конкуренции.

Т. е. в первой сноске указывайте автора, полное название, место, год издания, страницы, на которые ссылаетесь.

В дальнейшем в сноске следует писать: Там же. – С. 98.

Если сноска на данную работу дана после других источников, следует писать: Государственная политика: Учебное пособие. – С. 197. (без указания места и года издания).

Ссылки на Интернет даются с обязательной датой просмотра сайта, т. к. сайты часто обновляются и порой невозможно найти те материалы, которые использовались в реферате. Например: Федеральный закон от 14 ноября 2002 г. № 161-ФЗ «О государственных и муниципальных унитарных предприятиях» [электронный текстовый документ].

–URL: [http://www.ranatruda.ru/ot\\_biblio/normativ/data\\_normativ/11/11264/index.php](http://www.ranatruda.ru/ot_biblio/normativ/data_normativ/11/11264/index.php) [дата обращения: 13.11.2015].

Вполне возможно помещение всех сносок реферата в специальный раздел Примечания.

В конце реферата приводится библиографический список, составленный в алфавитном порядке в соответствии с требованиями к оформлению справочно-библиографического аппарата. Источники и литература должны быть оформлены на разных страницах. Следует указывать только те источники и литературу, которую студент действительно изучил.

Библиографический список и сноски оформляются в соответствии с действующими стандартами. Реферат может содержать приложения в форме схем, таблиц, образцов документов и другие изображения в соответствии с темой исследования.

При написании реферата должно быть использовано не менее 25 источников или единиц литературы (книг, статей, интернет-сайтов, документов и др.). Учебники, энциклопедические и справочные издания не являются основной литературой и не входят в круг этих 25 наименований.

Если в реферате студент желает привести небольшие по объему документы или отдельные разделы источников, касающиеся выбранной темы, различные схемы, таблицы, диаграммы, карты, образцы типовых и эксклюзивных документов и другую информацию по основам государственного и муниципального управления, то их можно привести в разделе Приложения. При этом каждое приложение должно быть пронумеровано и снабжено указанием, откуда взята информация для него.

Введение, заключение, новые главы, библиографический список, должны начинаться с нового листа.

Все страницы работы, включая оглавление и библиографический список, нумеруются по порядку с титульного листа (на нем цифра не ставится) до последней страницы без пропусков и повторений. Порядковый номер проставляется внизу страницы по центру, начиная с цифры 2.

В реферате желательно высказывание самостоятельных суждений, аргументов в пользу своей точки зрения на исследуемую проблему. При заимствовании материала из первоисточников обязательны ссылки на автора источника или интернет-ресурс, откуда взята информация. Реферат, значительная часть которого текстуально переписана из какого-либо источника, не может быть оценена на положительную оценку.

Текст реферата заключается датой его завершения и личной подписью студента.