Компонент ОПОП 01.03.02 Прикладная математика и информатика, направленность (профиль) «Системное программирование и компьютерные технологии»
наименование ОПОП
Б1.О.16.03
шифр дисциплины

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Дисциплины (модуля) **Защита информации**

Разработчик (и):
Л.Б. Сенецкая
ФИО
доцент
должность

к.э.н ,доцент
ученая степень, звание

Утверждено на заседании кафедры
информационных технологий,
наименование кафедры

протокол №__ от _____

Заведующий кафедрой ИТ
_____ Ляш О.И.
подпись ФИО

1. Критерии и средства оценивания компетенций и индикаторов их достижения, формируемых дисциплиной (модулем)

Код и наименование компетенции	Код и наименование индикатора(ов) достижения компетенции	Результаты обучения по дисциплине (модулю)			Оценочные средства текущего контроля	Оценочные средства промежуточной аттестации
		Знать	***Уметь***	***Владеть***		
ОПК-4 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ИД-1ОПК-4 Понимает особенности работы современных информационных технологий. ИД-2ОПК-4 Анализирует принципы работы современных информационных технологий. ИД-3ОПК-4 Использует современные информационные технологии для решения задач профессиональной деятельности.	особенности работы современных информационных технологий с учетом требований информационной безопасности	использовать современные информационные технологии для решения задач профессиональной деятельности с учетом требований информационной безопасности	Навыками выбора современных информационных технологий и программных средств, в том числе отечественного производства при решении задач профессиональной деятельности с учетом требований информационной безопасности	комплект заданий для выполнения лабораторных работ; .учет посещаемости; тестовые наборы	Результаты текущего контроля

2. Оценка уровня сформированности компетенций (индикаторов их достижения)

Показатели оценивания компетенций (индикаторов их достижения)	Шкала и критерии оценки уровня сформированности компетенции			
	Ниже порогового *(«неудовлетворительно»)*	**Пороговый** *(«удовлетворительно»)*	**Продвинутый** *(«хорошо»)*	**Высокий** *(«отлично»)*
Полнота знаний	Уровень знаний ниже минимальных требований. Имели место грубые ошибки.	Минимально допустимый уровень знаний. Допущены не грубые ошибки.	Уровень знаний в объёме, соответствующем программе подготовки. Допущены некоторые погрешности.	Уровень знаний в объёме, соответствующем программе подготовки.
Наличие умений	При выполнении стандартных заданий не продемонстрированы основные умения.	Продемонстрированы основные умения. Выполнены типовые задания	Продемонстрированы все основные умения. Выполнены все основные задания	Продемонстрированы все основные умения. Выполнены все основные и

	Имели место грубые ошибки.	с не грубыми ошибками. Выполнены все задания, но не в полном объеме (отсутствуют пояснения, неполные выводы)	с некоторыми погрешностями. Выполнены все задания в полном объёме, но некоторые с недочетами.	дополнительные задания без ошибок и погрешностей. Задания выполнены в полном объеме без недочетов.
Наличие навыков (владение опытом)	При выполнении стандартных заданий не продемонстрированы базовые навыки. Имели место грубые ошибки.	Имеется минимальный набор навыков для выполнения стандартных заданий с некоторыми недочетами.	Продемонстрированы базовые навыки при выполнении стандартных заданий с некоторыми недочетами.	Продемонстрированы все основные умения. Выполнены все основные и дополнительные задания без ошибок и погрешностей. Продемонстрирован творческий подход к решению нестандартных задач.
Характеристика сформированности компетенции	Компетенции фактически не сформированы. Имеющихся знаний, умений, навыков недостаточно для решения практических (профессиональных) задач.	Сформированность компетенций соответствует минимальным требованиям. Имеющихся знаний, умений, навыков в целом достаточно для решения практических (профессиональных) задач.	Сформированность компетенций в целом соответствует требованиям. Имеющихся знаний, умений, навыков достаточно для решения стандартных профессиональных задач.	Сформированность компетенций полностью соответствует требованиям. Имеющихся знаний, умений, навыков в полной мере достаточно для решения сложных, в том числе нестандартных, профессиональных задач.

3. Критерии и шкала оценивания заданий <u>текущего контроля</u>

3.1 <u>Критерии и шкала оценивания лабораторных работ</u>

Перечень лабораторных работ описание порядка выполнения и защиты работы, требования к результатам работы, структуре и содержанию отчета и т.п. представлены в методических материалах по освоению дисциплины (модуля) и в электронном курсе в ЭИОС МАУ.

Оценка/баллы	Критерии оценивания
Отлично	Задание выполнено полностью и правильно. Отчет по лабораторной/практической работе подготовлен качественно в соответствии с требованиями. Полнота ответов на вопросы преподавателя при защите работы.
Хорошо	Задание выполнено полностью, но нет достаточного обоснования или при верном решении допущена незначительная ошибка, не влияющая на правильную последовательность рассуждений. Все требования, предъявляемые к работе, выполнены.
Удовлетворительно	Задания выполнены частично с ошибками. Демонстрирует средний уровень выполнения задания на лабораторную/практическую работу. Большинство требований, предъявляемых к заданию, выполнены.
Неудовлетворительн	Задание выполнено со значительным количеством ошибок на низком уровне.

о	Многие требования, предъявляемые к заданию, не выполнены. ИЛИ Задание не выполнено.

4. Критерии и шкала оценивания результатов обучения по дисциплине (модулю) при проведении <u>промежуточной аттестации</u>

БИЛЕТ 1

1. Понятие информационной безопасности и защиты информации. Составляющие информационной безопасности
2. Классификация уязвимостей. Метод их ранжирования

Вопросы к экзамену

1. Цели и задачи информационной безопасности.
2. Аспекты информационной безопасности.
3. Уровни формирования режимов информационной безопасности.
4. Виды субъектов информационных отношений на предприятии.
5. Классификация информационных активов предприятия по степени конфиденциальности информации.
6. Защита персональных данных. Законодательная база .
7. Защита государственной тайны. Законодательная база.
8. Защита коммерческой тайны. Законодательная база.
9. Национальные интересы и безопасность России. Основные положения доктрины информационной безопасности
10. Понятие информационной войны. Особенности информационной войны. Понятие информационного превосходства.
11. Аспекты оценки доверенных систем в стандарте Оранжевая книга.
12. «Критерии оценки доверенных компьютерных систем» как оценочный стандарт.
13. Дискреционное и мандатное разграничение доступа. Особенности.
14. Сервисы и механизмы защиты в стандарте Рекомендации X.800.
15. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий» . Классификация систем по степени безопасности.
16. Виды угроз собственной информации.
17. Классификация источников угроз информационной безопасности.
18. Классификация уязвимостей информационной безопасности.
19. Административно- организационный уровень формирования режима информационной безопасности. Концепция информационной безопасности.
20. Модель неформального нарушителя.
21. Понятия идентификация, аутентификация. Методы и типы аутентификации.
22. Вредоносное программное обеспечение.
23. Средства антивирусной защиты
24. Антивирусные программы. Программы-детекторы. Программы-доктора.
25. Антивирусы-полифаги. Эвристические анализаторы.
26. Программы-ревизоры. Программы-фильтры.
27. Криптография.. История развития криптографии. Примеры шрифтов.
28. Шифр Цезаря. Шифр Атбаш
29. Квадрат Полибия, система Плейфера.
30. Шифрование, задачи шифрования, криптостойкость шифра
31. Шифрование симметричные и ассиметричные шрифты.

32. Виды удаленных атак, их краткая характеристика.
33. Модель ISO/OSI и сетевая безопасность.
34. Комплексная система защиты безопасности, базовые принципы формирвоания.
35. Классификация закладок. Причины защиты ПК от закладок. Аппаратные закладки.
36. Программные закладки. Классификация критериев вредоносного воздействия закладок.

Оценка	Критерии оценки ответа на экзамене
Отлично	Обучающийся глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, не затрудняется с ответом при видоизменении вопроса. Владеет специальной терминологией, демонстрирует общую эрудицию в предметной области, использует при ответе ссылки на материал специализированных источников, в том числе на Интернет-ресурсы.
Хорошо	Обучающийся твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, владеет специальной терминологией на достаточном уровне; могут возникнуть затруднения при ответе на уточняющие вопросы по рассматриваемой теме; в целом демонстрирует общую эрудицию в предметной области.
Удовлетворительно	Обучающийся имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, плохо владеет специальной терминологией, допускает существенные ошибки при ответе, недостаточно ориентируется в источниках специализированных знаний.
Неудовлетворительно	Обучающийся не знает значительной части программного материала, допускает существенные ошибки, нарушения логической последовательности в изложении программного материала, не владеет специальной терминологией, не ориентируется в источниках специализированных знаний. Нет ответа на поставленный вопрос.

Оценка, полученная на экзамене, переводится в баллы («5» - 20 баллов, «4» - 15 баллов, «3» - 10 баллов) и суммируется с баллами, набранными в ходе текущего контроля.

Итоговая оценка по дисциплине (модулю)	Суммарные баллы по дисциплине (модулю), в том числе	Критерии оценивания
Отлично	91 - 100	Выполнены все контрольные точки текущего контроля на высоком уровне. Экзамен сдан
Хорошо	81-90	Выполнены все контрольные точки текущего контроля. Экзамен сдан
Удовлетворительно	70- 80	Контрольные точки выполнены в неполном объеме. Экзамен сдан
Неудовлетворительно	69 и менее	Контрольные точки не выполнены или не сдан экзамен

5. Задания диагностической работы для оценки результатов обучения по дисциплине (модулю) в рамках внутренней и внешней независимой оценки качества образования

ФОС содержит задания для оценивания знаний, умений и навыков, демонстрирующих уровень сформированности компетенций и индикаторов их достижения в процессе освоения дисциплины (модуля).

Комплект заданий разработан таким образом, чтобы осуществить процедуру оценки каждой компетенции, формируемых дисциплиной (модулем), у обучающегося в письменной форме.

Содержание комплекта заданий включает тестовые задания

ВАРИАНТ 1

1. Информация может составлять коммерческую тайну, если
- содержится в учредительных документах;
*-к ней нет свободного доступа на законном основании;
-содержится в бухгалтерских балансах;
2. Правовое обеспечение информационной безопасности- это…
-документированные сведения, лежащие в основе решения задач, обеспечивающих функционирование системы;
*-Нормативные документы по ИБ, требования которых являются обязательными в рамках сферы действия каждого подразделения;
-широкое использование технических средств защиты информации;
3. Угрозой безопасности автоматизированных банковских систем не является:
фишинг;
*аутсорсинг;
хакерские атаки;
4. Что, из указанного ниже является принципами информационной безопасности (три варианта):
скрытость;
масштабируемость;
*системность;
*законность;
*открытость алгоритмов;
5. Вирусам изменяющие среду обитания:
черви;
троянские;
*полиморфные;
макровирусы;
6. Какие угрозы информационной безопасности являются преднамеренными:
неумышленное повреждение каналов связи;
некомпетентное использование средств защиты;
*поджег;
7. Что такое несанкционированный доступ?
Вход в систему без согласования с руководителем организации;
*доступ в систему в нарушение установленных в системе правил разграничения доступа;
Удаление данных без согласования с руководством;
8. Ботнеты- это
*сеть компьютеров, зараженных вредоносной программой, позволяющей удаленно управлять зараженными компьютерами;
сеть компьютеров, зараженных блоккерами;
сеть компьютеров, распространяющих сетевые черви;
9. Что, из указанного ниже является принципами информационной безопасности (три варианта):
скрытость;
масштабируемость;
*системность;
*законность;
*открытость алгоритмов;
10. Вирусам изменяющие среду обитания:
черви;
троянские;
*полиморфные;
макровирусы;
11. Какая наиболее яркая черта вируса «сетевой червь»?
распространяется через съемные носители;
*распространяется по сети;
саморепликация;

12. По числу компьютерных преступлений лидируют:
информационные системы образовательных учреждений;
*автоматизированные банковские системы;
корпоративные информационные системы в промышленности;
13. Программы, предназначенные для записи информации о нажатиях клавиш клавиатуры в специализированный журнал регистрации(log-файл),который впоследствии изучается установившим программу злоумышленником называются:
malware$
троянцы-бэкдоры;
*кейлоггеры;
14. Что, из указанного ниже является принципами информационной безопасности (три варианта):
скрытость;
масштабируемость;
*системность;
*законность;
*открытость алгоритмов;
15. Вирусам изменяющие среду обитания:
черви;
троянские;
*полиморфные;
макровирусы;

ВАРИАНТ 2

1. К какой главе УК РФ относятся ст.272,ст.273ст.,274 в области информационной безопасности?
27
25
*28
2. К понятию информационной безопасности не относиться:
надежность работы компьютеры;
*Природоохранные мероприятия;
сохранность ценных данных;
3. К активным угрозам относятся:
*разрушение или радиоэлектронное подавление линий связи, вывод из строя ПЭВМ или операционной системы;
попытка получения информации , циркулирующей в каналах связи, посредством их прослушивания;
копирование информации;
4. Что, из указанного ниже является принципами информационной безопасности (три варианта):
скрытость;
масштабируемость;
*системность;
*законность;
*открытость алгоритмов;
5. Вирусам изменяющие среду обитания:
черви;
троянские;
*полиморфные;
макровирусы;
6. В системах дистанционного банковского обслуживания используется следующий протокол, осуществляющий шифрование конфиденциальной информации-
http
*https
ftp
smtp
7 Что такое государственная тайна?
сведения о состоянии окружающей среды;

все сведения, которые хранятся в государственных базах данных;
*защищаемые государством сведения в различных областях, распространение которых может нанести ущерб безопасности РФ;
8. Не являются коммерческой тайной :
сведения о научных разработках;
*сведения, содержащиеся в документах, дающих право заниматься предпринимательской деятельностью;
сведения о персонале предприятия;
9. Что, из указанного ниже является принципами информационной безопасности (три варианта):
скрытость;
масштабируемость;
*системность;
*законность;
*открытость алгоритмов;
10. Вирусам изменяющие среду обитания:
черви;
троянские;
*полиморфные;
макровирусы;
11. Информационное оружие-это…?
комплекс мер направленных на изменение индивидуального и общественного сознания;
*комплекс методов, средств и технологий предназначенных для распространения дезинформации в системе формирования общественного сознания;
комплекс нормативно-правовой документации;
12 Гарантия того, что конкретная информация доступна только тому кругу лиц, для которых она предназначена- это…
*конфиденциальность;
целостность;
доступность;
аутентичность;
13 Обеспечение того, что информационная система ведет себя в нормальном и внештатном режиме так, как запланировано- это..
*надежность;
точность;
контролируемость;
устойчивость;
доступность;
14. Что, из указанного ниже является принципами информационной безопасности (три варианта):
скрытость;
масштабируемость;
*системность;
*законность;
*открытость алгоритмов;
15. Вирусам изменяющие среду обитания:
черви;
троянские;
*полиморфные;
макровирусы;

Шкала оценивания комплексного задания

Оценка (баллы)	**Критерии оценки**
5 «отлично»	90%< правильных ответов
4 «хорошо»	80% <правильных ответов<=90%
3 «удовлетворительно»	60% <правильных ответов<=81%
2 «неудовлетворительно»	правильных ответов<=60%