Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Воронежский государственный аграрный университет имени императора Петра I»

Гуманитарно-правовой факультет

Кафедра информационного обеспечения и моделирования агроэкономических систем

Утверждаю:
Заведующий кафедрой

_____
профессор А.В. Улезько

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине
Б1.В.ДВ.13.1 МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Направление подготовки:
Академический бакалавриат 44.03.04 Профессиональное обучение (по отраслям)

Профиль:
Информатика, вычислительная техника и компьютерные технологии

Содержание

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

Код	Содержание	Разделы дисциплины							
		1	2	3	4	5	6	7	8
ОПК-5	Способность самостоятельно работать на компьютере (элементарные навыки)	+	+	+	+	+	+	+	+

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

2.1. Шкала академических оценок освоения дисциплины

Вид оценки	Оценки			
Академическая оценка по 4-х балльной шкале	неудовлетворительно	удовлетворительно	хорошо	отлично

Вид оценки	Оценки	
Академическая оценка по 2-х бальной системе (зачет)	не зачтено	зачтено

2.2. Текущий контроль

Код	Планируемые результаты	Разделы дисциплины	Содержание требований в разрезе разделов дисциплины	Технология формирования	Форма оценочного средства (контроля)	Уровни		
						пороговый (удовл.)	повышенный (хорошо)	высокий (отлично)
ОПК -5	Знать: -методы защиты информации -аппаратные и программные средства защиты информации Уметь: - использовать методы, аппаратные и программные средства защиты информации для обеспечения информационной безопасности. Иметь навыки: - использования методов и средств для реализации системы защиты информации.	1, 2, 3, 4, 5, 6, 7, 8	Сформированные знания, умения и навыки	Аудиторные занятия, самостоятельная работа	Устный опрос, тестирование	Тесты из раздела 3.7.	Тесты из раздела 3.7.	Тесты из раздела 3.7.

2.3. Промежуточная аттестация

Код	Планируемые результаты	Технология формирования	Форма оценочного средства (контроля)	Уровни		
				пороговый (зачтено)		
ОПК-5	Знать: - методы защиты информации -аппаратные и программные средства защиты информации	Аудиторные занятия, самостоятельная работа	Зачет, тестирование	Вопросы из раздела 3.2. Тесты из раздела 3.7.		
	Уметь: - использовать методы, аппаратные и программные средства защиты информации для обеспечения информационной безопасности.	Аудиторные занятия, самостоятельная работа	Зачет, тестирование, практические задания.	Вопросы из раздела 3.2. Тесты из раздела 3.7.		
	Иметь навыки: - навыками использования методов и средств для реализации системы защиты информации.	Аудиторные занятия, самостоятельная работа	Зачет, устный опрос, практические задания.	Вопросы из раздела 3.2. Тесты из раздела 3.7.		

2.4. Критерии оценки на экзамене

Экзамен учебным планом не предусмотрен

2.5. Критерии оценки на зачете

Оценка экзаменатора, уровень	Критерии
Зачтено	Выполнил предусмотренные рабочей программой лабораторные задания и отчитался об их выполнении
Не зачтено	Не выполнил предусмотренные рабочей программой лабораторные задания или не отчитался об их выполнении

2.6. Критерии оценки на дифференцированном зачете (защита курсового проекта)

Не предусмотрены

2.7. Критерии оценки контрольной работы

Не предусмотрены

2.8.Критерии оценки устного опроса

Оценка	Критерии
Отлично	Студент четко выражает свою точу зрения по рассматриваемым вопросам, приводя соответствующие примеры
Хорошо	Студент хорошо владеет материалом, но допускает отдельные погрешности в ответе
Удовлетворительно	Студент демонстрирует существенные пробелы в знаниях основного учебного материала
Неудовлетворительно	Студент демонстрирует неумение даже с помощью преподавателя получить правильное решение задачи из числа предусмотренных рабочей программой учебной дисциплины

2.9. Критерии оценки тестов

Уровни освоения компетенций	Оценка	Критерии
Высокий	отлично	Содержание правильных ответов в тесте не менее 90%
Продвинутый	хорошо	Содержание правильных ответов в тесте не менее 75%
Пороговый	удовлетворительно	Содержание правильных ответов в тесте не менее 50%
Не сформированы	неудовлетворительно	Содержание правильных ответов в тесте менее 50%

2.10. Критерии оценки задач

Оценка	Критерии
Отлично	Студент выполнил работу согласно всем требованиям, проявил творческие способности при оформлении работ, существенно разобрался в вопросах решения задач
Хорошо	Студент выполнил работу согласно всем требованиям, однако имеются незначительные недоработки; проявил творческие способности при оформлении работ, разобрался в вопросах решения задач

Удовлетворительно	Студент демонстрирует существенные пробелы в знаниях, не совсем разобрался в вопросах решения задач.
Неудовлетворительно	Студент демонстрирует неумение даже с помощью преподавателя правильно выполнить поставленную задачу из числа предусмотренных рабочей программой учебной дисциплины

2.11. Критерии допуска к зачету

Выполнение плана лабораторных занятий, сдача итогового теста.

3. Типовые контрольные задания для оценки знаний, умений и навыков

3.1. Вопросы к экзамену

Не предусмотрены

3.2 Вопросы к зачету

1. Основные понятия и определения в области информационной безопасности
2. Определение информационной безопасности в свете информационных проблем современного общества
3. Основные составляющие информационной безопасности
4. Значение информационной безопасности для субъектов информационных отношений
5. Составляющие национальных интересов РФ в информационной сфере
6. Понятие и сущность защиты информации
7. Цели защиты информации
8. Концептуальная модель информационной безопасности
9. Законодательство РФ в области информационной безопасности
10. Государственные информационные ресурсы и защита государственной тайны как особого вида защищаемой информации
11. Защита конфиденциальной информации, в том числе интеллектуальной собственности и коммерческой тайны
12. Нормативно-правовая база защиты информации: основные законы РФ в области защиты информации и указы Президента РФ
13. Предмет защиты информации
14. Информация как объект права собственности
15. Объект защиты информации
16. Случайные угрозы
17. Преднамеренные угрозы
18. Модель гипотетического нарушителя информационной безопасности
19. Анализ компьютерных преступлений
20. Несанкционированный доступ к информации и его цели
21. Компьютерные вирусы
22. Шпионские программные закладки
23. Основные принципы построения системы защиты
24. Методы защиты информации
25. Основные понятия и определения
26. История развития криптографии
27. Основные задачи криптологии - криптография и криптоанализ
28. Классификация криптографических методов
29. Анализ основных криптографических методов защиты информации: методы подстановки
30. Анализ основных криптографических методов защиты информации: методы перестановки;

31. Анализ основных криптографических методов защиты информации: гаммирование
32. Современные симметричные криптографические системы: системы с секретным ключом;
33. Современные симметричные криптографические системы: стандарт шифрования DES;
34. Современные симметричные криптографические системы: стандарт шифрования ГОСТ 28147
35. Асимметричные криптографические системы: системы с открытым ключом;
36. Асимметричные криптографические системы: стандарт шифрования RSA;
37. Электронная цифровая подпись
38. Системы предотвращения вторжений
39. Межсетевые экраны, классы их защищенности.
40. Понятие виртуальных частных сетей

3.3 Вопросы к дифференцированному зачету (защита курсового проекта)

Не предусмотрены

3.4 Задания для контрольной работы

Не предусмотрены

3.5 Вопросы к устному опросу

1. Дайте определение понятию информационная безопасность.
2. Перечислите основные составляющие информационной безопасности.
3. Какое значение имеют составляющие информационной безопасности для субъектов информационных отношений?
4. Каковы интересы РФ в информационной сфере?
5. Определите источники угроз информационной безопасности РФ и постройте их классификацию.
6. Перечислите основные методы обеспечения информационной безопасности РФ.
7. Какие основные проблемы международного сотрудничества стоят на повестке дня сегодня?
8. Каково, на ваш взгляд, положение дел в области мировой информационной безопасности сегодня?
9. Проанализируйте различные определения понятия «защита информации» и «информационная безопасность», заполните таблицу.
10. Что общего можно обнаружить во всех определениях? О чем это свидетельствует?
11. Дайте определение понятию защита информации.
12. Что понимается под термином безопасность информации?
13. Что включает в себя защита информации?
14. Какие цели преследует защита информации?
15. Какое место занимает защита информации в информационной безопасности?
16. Определите предмет защиты информации.
17. Сформулируйте основные свойства информации.
18. Дайте определение конфиденциальной информации.
19. Перечислите уровни секретности государственной тайны.
20. Раскройте сущность основных подходов к измерению количества информации.
21. Раскройте сущность информации как объекта права собственности.
22. Раскройте сущность объекта защиты.
23. Определите понятие угрозы информационной безопасности (ИБ).
24. Охарактеризуйте случайные угрозы ИБ.
25. Охарактеризуйте преднамеренные угрозы ИБ.
26. Определите понятия нарушителя ИБ и злоумышленника.
27. Какие предположения выдвигаются при разработке модели гипотетического нарушителя ИБ объекта.
28. На основании чего строится модель гипотетического нарушителя ИБ?
29. Какие категории персонала объекта могут быть внутренними нарушителями ИБ объекта?
30. Какие лица могут быть нарушителями ИБ объекта из числа посторонних лиц?
31. Назовите основные мотивы нарушений ИБ.
32. Дайте определение компьютерного преступления и охарактеризуйте их виды
33. Определите понятия вредоносного программного обеспечения и компьютерного вируса
34. Перечислите основные классы компьютерных вирусов
35. В чем заключаются различия между понятиями компьютерного вируса и шпионской программной заклад-

ки?
36. Назовите основные методы внедрения программных закладок
37. Дайте характеристику основных моделей воздействия программных закладок на компьютер и компьютерную сеть
38. В чем различия троянских программ и программных закладок?
39. Дайте характеристику действий основных разновидностей троянских программ
40. Назовите и охарактеризуйте методы обнаружения вирусов
41. Перечислите виды и назначения антивирусных программ
42. Какими действиями можно предотвратить вирусную атаку?
43. Назовите основополагающие документы по ИБ в РФ.
44. Что является предметом правового регулирования в области ИБ?
45. Назовите задачи обеспечения ИБ, сформулированные в Концепции национальной безопасности РФ
46. Какой закон является базовым в области защиты информации, и какие отношения он регламентирует?
47. Назовите категории государственных информационных ресурсов
48. Какая информация может быть отнесена к категории конфиденциальной?
49. Определите данные, которые могут быть отнесены к персональным данным
50. Назовите статьи УК РФ, предусматривающие ответственность за совершение компьютерных преступлений
51. Сформулируйте основные принципы построения системы защиты информации.
52. Какие уровни задействованы в обеспечении информационной безопасности?
53. Что представляет собой политика безопасности организации?
54. Что входит в анализ рисков?
55. Что представляет собой программа безопасности организации?
56. Перечислите основные модели защиты информации и их особенности.
57. В чем заключается сущность методов защиты от случайных угроз?
58. Дайте определение понятиям идентификации и аутентификации.
59. Перечистите основные виды аутентификации.
60. В чем заключается повышение надежности и отказоустойчивости информационных систем?
61. Какую роль играет подготовленность персонала в построении системы защиты информации?
62. Какие методы и средства используются для организации противодействия традиционным методам шпионажа и диверсий?
63. Раскройте особенность построения защиты от несанкционированного доступа
64. Какие методы защиты информации относятся к криптографическим?
65. Дайте определение криптологии.
66. Какие три основных периода криптологии вы знаете?
67. Объясните понятие «криптологический алгоритм».
68. Что такое криптография?
69. Приведите основную классификацию криптографических методов.
70. Какова суть преобразований перестановки и замены?
71. Что собой представляют шифрование и дешифрование?
72. Дайте определение аналитическому преобразованию, гаммированию и комбинированному шифрованию.
73. Что такое системы с открытыми ключами?
74. Приведите структурную схему процесса шифрования с открытым ключом.
75. Дайте определение стойкости криптосистемы.
76. Приведите основные программно-аппаратные реализации шифров.
77. В чем заключается суть DES-алгоритма? Каковы его особенности?
78. В каких режимах может работать DES-алгоритм?
79. Дайте описание отечественного алгоритма криптографического преобразования данных (ГОСТ 28147 - 89) и его отличительных особенностей.
80. Какими характеристиками оценивается стойкость криптографических систем?
81. В чем заключается суть электронной цифровой подписи?
82. Как проверяется целостность сообщения?
83. Дайте определение межсетевого экрана.
84. Назовите типы межсетевых экранов.
85. Объясните различия между межсетевыми экранами разных типов.
86. Объясните преимущества виртуальных сетей.
87. Назовите компоненты виртуальной сети.
88. Объясните назначение димилитаризированной зоны (DMZ).
89. Назовите цели использования системы обнаружения вторжений.
90. Назовите основные типы систем обнаружения вторжений.
91. Укажите преимущества и недостатки NIDS.

3.6 Вопросы к коллоквиуму

Не предусмотрены

3.7 Тестовые задания

3.7.1 Количество тестовых вопросов:

всего	167
по разделу 1	15
по разделу 2	15
по разделу 3	15
по разделу 4	25
по разделу 5	17
по разделу 6	30
по разделу 7	35
по разделу 8	12

3.7.2 Структура тестов и время на выполнение:

Тесты по отдельным разделам должны включать следующее количество вопросов:

Номер раздела	Количество вопросов	Время на выполнение теста, мин
Раздел №1	45	45
Раздел №2		
Раздел №3		
Раздел №4	25	25
Раздел №5	17	15
Раздел №6	30	30
Раздел №7	35	35
Раздел №8	12	10

Итоговый тест должен содержать 45 вопросов:

Вид теста	Количество вопросов							Время на выполнение теста
	из раздела №1, №2, №3	из раздела №4	из раздела №5	из раздела №6	из раздела №7	из раздела №8	Всего	
Итоговый	12	7	5	8	10	3	45	45

3.7.3 Содержание тестовых заданий

Разделы №1, №2, №3: Информационная безопасность, Общее содержание защиты информации, Угрозы информационной безопасности

1. Информация, несанкционированное копирование, хищение, разглашение (распространение, опубликование), модификация, уничтожение или использование которой может нанести существенный моральный или материальный ущерб ее собственнику или владельцу, а также третьей стороне, интересы которой данная информация затрагивает, называется:
   - критичной информацией
   - информацией общего доступа
   - персональными данными
2. Укажите категории ценности информации с точки зрения информационной безопасности:
   - конфиденциальность
   - целостность

статичность
доступность
аутентичность
адекватность
аппелируемость

3. Категория ценности информации, определяющая гарантию того, что источником информации является именно то лицо, которое заявлено как ее автор, называется:
   аутентичность
   аппелируемость
   достоверность
4. Аутентичность связана:
   с проверкой прав доступа
   с доказательством авторства документа
   с изменением авторства документа
   с контролем целостности данных
5. Категория ценности информации, гарантирующая, что при необходимости можно доказать, что автором сообщения является именно заявленный человек, и не может являться никто другой, называется:
   аутентичность
   аппелируемость
   достоверность
6. Убытки, которые могут возникнуть вследствие внесения изменений в информацию, если факт модификации не был обнаружен, называются:
   стоимость скрытого нарушения целостности
   стоимость утраты
   стоимость потери конфиденциальности
7. Потенциальные убытки, которые понесет владелец информации, если к ней получат неавторизованный доступ сторонние лица, называются:
   стоимость скрытого нарушения целостности
   стоимость утраты
   стоимость потери конфиденциальности
8. Ущерб от полного или частичного разрушения информации называется:
   стоимость скрытого нарушения целостности
   стоимость утраты
   стоимость потери конфиденциальности
9. Что не является преднамеренным воздействием на информационную систему:
   подбор пароля
   перехват информации
   хищение информации
   модификация информации
   стихийные бедствия
10. Что не является причиной случайных воздействии на информационную систему:
    подбор пароля
    отказы и сбои аппаратуры
    ошибки персонала
    помехи в линиях связи из-за воздействий внешней среды
11. Укажите пути несанкционированной передачи информации:
    хищение носителей информации
    негласный просмотр информации, отображенной на мониторе ЭВМ
    подключение к устройствам передачи, обработки и хранения информации специализированных аппаратных средств
    внедрение резидентных программ

регистрация и анализ побочных электромагнитных излучений средств электронно-вычислительной техники, связи и телекоммуникаций
установка подслушивающих и передающих устройств
распространение информации ее владельцем

12. Укажите составляющие информационной безопасности:
доступность информации
целостность информации
конфиденциальность информации
проверка прав доступа к информации
выявление нарушителей

13. Конфиденциальность информации гарантирует:
доступность информации только тому кругу лиц, для кого она предназначена
защищенность информации от потери
доступность информации только автору

14. Потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, утрате целостности, конфиденциальности или доступности информации называется:
угрозой информационной безопасности
несанкционированным доступом к информации
фальсификацией информации

15. Защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации называется:
информационной безопасностью
компьютерной безопасностью
защитой информации
защитой государственной тайны

16. Комплекс средств и методов, направленных на предотвращение угроз информационной безопасности и устранение их последствий, называется:
защитой информации
компьютерной безопасностью
информационной безопасностью
защитой государственной тайны

17. Что из перечисленного является задачей информационной безопасности:
защита технических и программных средств информатизации от ошибочных действий персонала
устранение неисправностей аппаратных средств
устранение последствий стихийных бедствий
восстановление линий связи

18. Доступность информации гарантирует:
получение требуемой информации за определенное время
неизменность информации в любое время
получение требуемой информации за неопределенное время
защищенность информации от возможных угроз

19. Целостность информации гарантирует:
существование информации в исходном виде
принадлежность информации автору
доступ информации определенному кругу пользователей
защищенность информации от несанкционированного доступа

20. Процесс распознавания пользователя автоматизированной системой, для чего предъявляется уникальное имя, называется:
идентификацией

аутентификацией
сертификацией

21. Процедура проверки подлинности, предназначенная для подтверждения истинности пользователя, предъявившего идентификатор, называется:
идентификацией
аутентификацией
контролем доступа

22. Идентификация и аутентификации применяются:
для ограничения доступа случайных и незаконных субъектов к информационной системе
для защиты от компьютерных вирусов
для обеспечения целостности данных

23. Присвоение субъектам идентификаторов и (или) сравнение предъявляемых идентификаторов с перечнем идентификаторов, владельцы которых допущены к информационной системе, называется:
идентификацией
аутентификацией
аутентичностью
конфиденциальностью

24. Результатом реализации угроз информационной безопасности может быть:
уничтожение устройств ввода-вывода информации
несанкционированный доступ к информации
изменение конфигурации периферийных устройств

25. Угроза перехвата данных может привести:
к нарушению доступности данных
к отказу в обслуживании
к нарушению конфиденциальности данных

26. Идентификация и аутентификация применяются:
для повышения физической защиты информационной системы
для ограничения доступа случайных и незаконных субъектов к информационной системе
для защиты от компьютерных вирусов
для обеспечения целостности данных

27. Подберите слово к данному определению: ??? - проверка принадлежности субъекту предъявленного им идентификатора и подтверждение его подлинности.
аутентификация
идентификация
целостность
конфиденциальность

28. Подберите слово к данному определению : ??? - присвоение субъектам личного идентификатора и сравнение его с заданным.
аутентификация
идентификация
аутентичность
конфиденциальность

29. Что из перечисленного является составляющей информационной безопасности?
целостность информации
несанкционированный доступ к информации;
санкционированный доступ к информации;
антивирусная защита

30. Одной из задач информационной безопасности является ??? — это совокупность методов и средств, предназначенных для ограничения доступа к ресурсам

контроль доступа
сертификация
секретность

31. Под информационной безопасностью (безопасностью информации) понимается:
комплекс организационно-технических мероприятий, обеспечивающих сохранность информационных ресурсов;
состояние, при котором отсутствуют явные и скрытые угрозы информационным ресурсам;
состояние защищенности информационной среды общества

32. Что такое угроза?
потенциально или реально существующие воздействия на информационную систему, приводящие к материальному или моральному ущербу;
воздействие, нанесшее ущерб информационной системе;
достоверные сведения о злоумышленных действиях в отношении информационной системы.

33. Бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена – это:
разглашение;
утечка;
несанкционированный доступ.

34. Умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним – это:
разглашение;
утечка;
несанкционированный доступ.

35. Противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым секретам –это:
разглашение;
утечка;
несанкционированный доступ.

36. В чем выражаются угрозы информационной безопасности
в нарушении конфиденциальности, целостности и доступности;
в несанкционированном разглашении информации;
в уничтожении информации;
в незаконном изменении (модификации) информации.

37. Мероприятия по формированию осознанного отношения сотрудников к обеспечению информационной безопасности относятся к:
предупреждению угроз;
выявлению угроз;
локализации угроз;
ликвидации последствий угроз.

38. Накопление сведений об угрозах информационной безопасности и их аналитическая обработка относится к:
предупреждению угроз;
выявлению угроз;
локализации угроз;
ликвидации последствий угроз.

39. Действия, направленные на устранение действующей угрозы и конкретных преступных действий относятся к:
предупреждению угроз;
выявлению угроз;
локализации угроз;

ликвидации последствий угроз.

40. Действия по восстановлению состояния, предшествовавшего возникновению угрозы, относятся к:
    предупреждению угроз;
    выявлению угроз;
    локализации угроз;
    ликвидации последствий угроз.
41. Основными мероприятиями по защите от разглашения является:
    разработка перечня сведений, составляющих коммерческую тайну предприятия.
    доведение перечня сведений, составляющих коммерческую тайну до каждого сотрудника, допущенного к ним, с обязательством этого сотрудника сохранять коммерческую тайну.
    контроль за сохранностью коммерческих секретов.
    все, перечисленные выше мероприятия.
42. Защита от утечки конфиденциальной информации сводится к:
    выявлению, учету и контролю возможных каналов утечки в конкретных условиях;
    проведению организационных, организационно-технических и технических мероприятий по ликвидации каналов утечки;
    комплексное выполнение мероприятий.
43. Защита от несанкционированного доступа к конфиденциальной информации обеспечивается выполнением:
    только организационных мероприятий;
    только технических мероприятий;
    организационных и технических мероприятий.
44. Определение состояния технической безопасности объекта относится к:
    организационным мероприятиям;
    техническим мероприятиям;
    организационно-техническим мероприятиям.
45. Какой из принципов нецелесообразно использовать при организации защиты информации;
    принцип коллективной ответственности;
    принцип персональной ответственности;
    принцип максимального ограничения допуска к информации.

Раздел №4. Компьютерные преступления и их особенности

1. Уголовно наказуемые общественно опасные действия, в которых машинная информация является объектом посягательства, называют:
    компьютерным преступлением
    несанкционированным действием
    компьютерным мошенничеством
2. Любая программа, написанная с целью нанесения ущерба или использования ресурсов атакуемого компьютера, называется:
    вредоносной программой
    компьютерным вирусом
    программной закладкой
3. Класс программ, способных к саморазмножению и самомодификации в работающей вычислительной среде и вызывающих нежелательные для пользователей действия, называется:
    компьютерным вирусом
    программной закладкой
    троянской программой
4. Укажите последовательность этапов жизненного цикла компьютерного вируса:
    внедрение (инфицирование)
    инкубационный период

саморазмножение (репродуцирование)
выполнение специальных функций
проявление

5. По среде обитания компьютерные вирусы подразделяют на:
   файловые вирусы
   загрузочные вирусы
   файлово-загрузочные вирусы
   сетевые вирусы
   полиморфные вирусы
   стелс-вирусы
6. Достаточно трудно обнаружимые вирусы, не имеющие сигнатур, то есть не содержащие ни одного постоянного участка кода, это:
   полиморфик-вирусы
   стелс-вирусы
   макро-вирусы
   конструкторы вирусов
7. Вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям:
   фишинг
   фарминг
   кардинг
   скимминг
8. ??? – это вирусы, заражающие файлы некоторых систем обработки документов (MS Word, MS Excel), которые имеют встроенные макро-языки
   macro-вирусы
   стелс-вирусы
   полиморфик-вирусы
9. ??? маскируют свое присутствие путем перехвата обращений ОС к пораженным файлам, секторам и переадресуют ОС к незараженным участкам
   macro-вирусы
   стелс-вирусы
   полиморфик-вирусы
10. ??? - это компьютерные вирусы, которые распространяются в компьютерных сетях и не изменяют файлы или секторы на дисках
    macro-вирусы
    вирусы-черви
    полиморфик-вирусы
11. Какой из вирусов при инфицировании компьютера оставляет в оперативной памяти свою часть, которая затем перехватывает обращения операционной системы к объектам заражения и внедряется в них?
    нерезидентный вирус
    файловый вирус
    резидентный вирус
    загрузочный вирус
12. Самошифрование и полиморфичность используются для:
    саморазмножения вируса
    максимального усложнения процедуры обнаружения вируса
    расшифровки тел вируса
    для скрытия действий антивирусной программы
13. Одним из наиболее эффективных способов борьбы с вирусами является:
    использование антивирусного программного обеспечения
    профилактика компьютерных вирусов

ограничение доступа пользователей к ЭВМ
шифрование данных

14. ??? - это программа, скрытно внедренная в защищенную систему и позволяющая злоумышленнику, путем модификации свойств системы защиты, осуществлять несанкционированный доступ к ресурсам системы
    программная закладка
    троянская программа
    стелс-вирус
15. К деструктивным действиям, осуществляемым программными закладками относятся:
    копирование конфиденциальной информации
    изменение алгоритмов функционирования системных, прикладных и служебных программ
    навязывание определенных режимов работы
    уменьшают объем свободной памяти на диске в результате своего распространения
    снижают эффективность функционирования компьютерной системы
16. Сопоставьте вид программной закладки с ее действием:
    L1: программные закладки-имитаторы
    L2: замаскированные программные закладки
    L3:
    R1: интерфейс совпадает с интерфейсом некоторых служебных программ, требующих ввести конфиденциальную информацию (пароль, криптографический ключ, номер кредитной карточки)
    R2: имитируют программные средства оптимизации работы ПК (файловые архиваторы, дисковые дефрагментаторы) или программы игрового и развлекательного назначения
    R3: проникают в компьютерную систему через такие подсистемы как электропитание, стабилизация и т.д.
17. Сопоставьте вид модели программных закладок с ее воздействия на компьютерную систему:
    L1: модель «перехват»
    L2: модель «искажение»
    L3: модель «уборка мусора»
    L4: модель «наблюдение»
    L5:
    R1: программная закладка внедряется в ПЗУ, системное ПО или прикладное ПО и сохраняет всю или выбранную информацию, вводимую с внешних устройств или выводимую на них
    R2: программная закладка изменяет информацию, которая записывается в память ПК в результате работы программ, либо подавляет/инициирует возникновение ошибочных ситуаций в ПК
    R3: программная закладка направлена на сохранение временных копий файлов или фрагментов файлов после их удаления
    R4: программная закладка встраивается в сетевое ПО и может следить за всеми процессами обработки информации в компьютерной системе
    R5: программная закладка позволяет получать доступ к информации, перехваченной другими программными закладками
18. Программа с известными ее пользователю функциями, в которую были внесены изменения, чтобы, помимо этих функций, она могла втайне от него выполнять некоторые другие (разрушительные) действия, называется:
    троянской программой
    программной закладкой
    компьютерным вирусом

19. ??? – это компьютерная программа, которая выявляет, предотвращает и выполняет определенные действия, чтобы блокировать или удалять вредоносные программы:
    Антивирусная программа
    Программа обнаружения вторжений
    Программная закладка
20. Сопоставьте вид антивирусной программы с ее назначением:
    L1: Детекторы (сканеры)
    L2:Доктора (фаги, полифаги)
    L3: Ревизоры
    L4:Фильтры (Сторожа)
    L5: Специальные вакцины
    L6: Блокировщики
    L7:
    R1: Обнаружение вирусов
    R2: Обнаружение и уничтожение вирусов
    R3: Контроль путей распространения вирусов
    R4: Контроль подозрительных на вирус операций
    R5: Обработка файлов и загрузочных секторов на устойчивость к вирусам
    R6: Ограничение распространения вирусов
    R7: Перемещение подозрительных файлов в карантин
21. Укажите методы обнаружения компьютерных вирусов:
    Сканирование
    Обнаружение изменений
    Эвристический анализ
    Использование резидентных сторожей
    Вакцинация
    Аппаратно-программные антивирусные средства
    Аналитическое преобразование
    Гаммирование
22. Сопоставьте методы обнаружения компьютерных вирусов с их действием:
    L1: метод сканирования
    L2: метод обнаружения изменений
    L3: эвристический анализ
    L4: метод использования резидентных сторожей
    L5:
    R1: поиск сигнатуры (постоянной опознавательной части) вируса
    R2: программы - ревизоры определяют и запоминают характеристики областей на дисках, затем сравниваются с хранящимися характеристиками
    R3: проверка возможных сред обитания вирусов и выявление команд, характерных для вирусов
    R4: постоянно отслеживают все действия остальных программ и при выполнении подозрительных действий выдается сообщение
    R5: создание специального модуля для контроля целостности программы (контрольная сумма)
23. ??? - комплекс программных или аппаратных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами. Позволяет блокировать нежелательный сетевой трафик, обеспечивает невидимость ПК в сети с целью предотвращения кибер атак:
    Сетевой экран (firewall)
    Маршрутизатор
    Интернет-шлюз
24. «Маски» (сигнатуры) вирусов используются:

для поиска известных вирусов
для создания известных вирусов
для уничтожения известных вирусов
для размножения вирусов

25. Укажите основные функции антивирусных программ:
сканирование памяти и содержимого дисков по расписанию и в режиме реального времени
выборочное сканирование файлов с измененными атрибутами
сканирование архивных файлов
распознавание поведения, характерного для компьютерных вирусов
автоматическое обновление антивирусных баз посредством Internet
фильтрация трафика Internet для выявления вирусов в программах и документах, передаваемых посредством протоколов FTP, HTTP
сбор адресов электронной почты на компьютере с последующей передачей их адресату через электронную почту, HTTP, FTP или другими способами
несанкционированная пользователем загрузка и установка на компьютере программ рассылки спама или рекламных систем

Раздел №5. Законодательные аспекты информационной безопасности в РФ

1. Основополагающими документами по информационной безопасности в РФ являются:
Конституция РФ
Концепция национальной безопасности
Уголовный Кодекс
Закон об информационной безопасности
2. Укажите документ, гарантирующий тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ст. 23, ч. 2); право свободно искать, получать, передавать, производить и распространять информацию любым законным способом (ст. 29, ч. 4); свободу массовой информации (ст. 29, ч. 5):
Конституция РФ
Концепция национальной безопасности
Уголовный Кодекс
Закон об информационной безопасности
3. Какой документ определяет важнейшие задачи обеспечения информационной безопасности РФ:
Конституция РФ
Концепция национальной безопасности
Уголовный Кодекс
Закон об информационной безопасности
4. Укажите сведения, имеющие конфиденциальный характер:
персональные данные
тайна следствия и судопроизводства
служебная тайна
профессиональная тайна
коммерческая тайна
сведения о сущности изобретения
план приема студентов в вуз
уставные документы бюджетной организации
5. Сколько категорий государственных информационных ресурсов определяет Закон РФ «Об информации, информационных технологиях и о защите информации» от 27.08.2006 г. № 149-ФЗ?
Три
Четыре
Два

Пять

6. Документированная информация, правовой режим которой установлен специальными нормами действующего законодательства в области государственной, коммерческой, промышленной и другой общественной деятельности, называется:
   конфиденциальной информацией
   персональными данными
   государственной тайной
7. Любая информация, с помощью которой можно однозначно идентифицировать физическое лицо, является:
   конфиденциальной информацией
   персональными данными
   информацией с ограниченным доступом
8. Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ, относятся к:
   государственной тайне
   документированной информации ограниченного доступа
   служебной тайне
9. Неправомерный доступ к компьютерной информации наказывается штрафом:
   от пяти до двадцати минимальных размеров оплаты труда
   от двухсот до пятисот минимальных размеров оплаты труда
   от ста пятидесяти до двухсот минимальных размеров оплаты труда
   до трехсот минимальных размеров оплаты труда
10. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети наказывается ограничением свободы на срок:
   до года
   до двух лет
   до пяти лет
   до трех месяцев
11. Создание, использование и распространение вредоносных программ для ЭВМ наказывается:
   лишением свободы до года
   штрафом до двадцати минимальных размеров оплаты труда
   лишением свободы на срок до 3 лет со штрафом в размере от 200 до 500 минимальных размеров оплаты труда
   исправительными работами до пяти лет
12. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети наказывается:
   штрафом до ста минимальных размеров оплаты труда
   ограничением свободы
   арестом на срок от 3 до 6 месяцев
   штрафом до пятисот минимальных размеров оплаты труда
13. Что такое доктрина информационной безопасности РФ
   совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации;
   совокупность нормативных актов, обязательных для выполнения всеми хозяйствующими субъектами.
   совокупность документов, регламентирующих организационно-технические мероприятия по обеспечению информационной безопасности Российской Федерации.
14. Какие из указанных мероприятий защиты информации относятся к правовым?
   организация режима и охраны;
   разработка ведомственной нормативной документации;

охрана оборудования, продукции, финансов и информации

15. Право разрешать или ограничивать доступ к информации и определять условия такого доступа принадлежит:
    органам законодательной власти;
    любому юридическому лицу;
    обладателю информации;
    органам исполнительной власти
16. Перечень сведений конфиденциального характера определен:
    Указом Президента РФ от 6 марта 1997 г. № 188;
    Федеральным законом от 27 июля 2006 г. N 149-ФЗ;
    Указом Президента РФ от 30 ноября 1995 г. N 1203.
17. Перечень сведений, доступ к которым не может быть ограничен определен:
    Федеральным законом от 27 июля 2006 г. N 149-ФЗ;
    Указом Президента РФ от 6 марта 1997 г. № 188;
    Указом Президента РФ от 30 ноября 1995 г. N 1203.

Раздел №6. Системное обеспечение защиты информации

1. Что не рассматривается в политике безопасности?
    требуемый уровень защиты данных
    роли субъектов информационных отношений
    анализ рисков
    защищенность сотрудников
2. Совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов, называется:
    политикой безопасности;
    информационной политикой;
    информационной безопасностью;
    защитой информации
3. Стратегию организации в области информационной безопасности, меру внимания и количество ресурсов, которые руководство считает целесообразным выделить для обеспечения информационной безопасности, определяет:
    политика безопасности
    концепция безопасности
    стратегия безопасности
4. На каком из уровней обеспечения информационной безопасности разрабатывается политика безопасности:
    информационном
    административном
    законодательно-правовом
    программно-техническом
5. Что не является содержанием административного уровня обеспечения информационной безопасности:
    разработка политики безопасности
    проведение анализа угроз и расчета рисков
    выбор механизмов обеспечения информационной безопасности
    внедрение механизмов безопасности
6. Какой из уровней обеспечения информационной безопасности включает комплекс мероприятий, реализующих практические механизмы защиты информации:
    законодательно-правовой
    процедурный
    административный
    программно-технический

7. Какой из перечисленных уровней не относится к уровням обеспечения информационной безопасности:
   информационный
   законодательно-правовой
   административный (организационный)
   программно-технический
8. Какие из указанных мероприятий защиты информации относятся к организационным?
   организация работы по анализу внутренних и внешних угроз конфиденциальной информации и выработке мер по обеспечению ее защиты;
   выявление каналов утечки информации на разных объектах и в помещениях;
   разработка специальных законов, полностью относящиеся к конкретным сферам отношений, отраслям хозяйства, процессам.
9. Какие из указанных мероприятий защиты информации относятся к инженерно-техническим?
   организация использования технических средств сбора, обработки, накопления и хранения конфиденциальной информации;
   организация работы по проведению систематического контроля за работой персонала с конфиденциальной информацией;
   поиск и обнаружение средств промышленного шпионажа.
10. Одним из важнейших организационных мероприятий является:
   организация режима и охраны;
   создание специальных штатных служб защиты информации;
   организация работы с персоналом
11. Возможности несанкционированного использования конфиденциальных сведений в значительной мере обусловливаются:
   техническими аспектами;
   злоумышленными действиями;
   небрежностью и халатностью пользователей или персонала защиты.
12. Система защиты информации – это:
   организованная совокупность специальных органов, средств, методов и мероприятий, обеспечивающих защиту информации от внутренних и внешних угроз
   система средств инженерно-технической защиты, обеспечивающая приемлемый уровень информационной безопасности.
   специальные подразделения, выполняющие мероприятия по защите информации
13. К недостаткам аппаратных средств инженерно-технической защиты относится:
   высокая стоимость;
   массо-габаритные характеристики;
   недостаточная гибкость.
14. К достоинствам программных средств инженерно-технической защиты относится:
   низкая стоимость;
   длительный период гарантированного использования;
   быстродействие.
15. Началу работ по созданию или совершенствованию системы защиты информации (СЗИ) предшествует:
   разработка приказа на проведение работ по созданию СЗИ
   определение перечня недостатков действующей СЗИ / требованиям к новой СЗИ;
   формирование списка подрядчиков, привлекаемых к созданию / реконструкции СЗИ
16. Мероприятия по созданию СЗИ начинаются:
   с оценки уязвимости информации, доступности ее для средств злоумышленника;
   анализ состава и содержания конфиденциальной информации, циркулирующей на конкретном объекте защиты;

анализ ценности информации для предприятия (организации) с позиций возможного ущерба от ее получения конкурентами

17. Информационная модель предприятия формируется после окончания
    анализа состава и содержания конфиденциальной информации
    анализа ценности информации
    оценки уязвимости информации
18. Организационно-функциональная схема СЗИ формируется на этапе:
    оценки затрат на разработку новой системы защиты информации;
    разработки организационных мер защиты информации;
    установления персональной ответственности за сохранность информации.
19. Программа обучения сотрудников формируется на этапе:
    проведения мотивационных мероприятий;
    реализации технологии защиты информации;
    приема в опытную эксплуатацию новой СЗИ.
20. Профили конфиденциальности сотрудников и линейных подразделений формируются на этапе:
    реализации технологии защиты информации
    установления персональной ответственности за сохранность информации.
    разработки организационных мер защиты информации;
21. Аналитический обзор действующей СЗИ формируется на этапе:
    оценки уязвимости информации;
    исследования действующей системы защиты информации
    оценки затрат на разработку новой системы защиты информации.
22. Контроль эффективности защиты необходимо начинать
    с проверки организационно-режимных средств и мероприятий
    с проверки эффективности системы противодействия
    с тестирования защиты от НСД
23. Что является определяющим при оценке эффективности системы защиты?
    соответствие уровня защиты степени важности информации;
    соответствие уровня защиты объемам обрабатываемой информации;
    соответствие уровня защиты условиям проекта.
24. К общим критериям ценности документов относят:
    происхождение документа;
    значимость описываемой проблемы;
    принципиальная новизна;
    степень отражения технологического уровня описываемой предметной области.
25. К специфическим критериям ценности документов относят:
    экономическая эффективность внедрения результатов исследования или технической идеи;
    содержание документа;
    внешние особенности документа

Раздел №7. Криптографические методы защиты информации

1. ### - это наука о методах преобразования (шифрования) информации с целью ее защиты от несанкционированного доступа
2. ### - это наука (и практика ее применения) о методах и способах расшифрования информации без знания ключей
3. ??? - набор средств и методов сокрытия факта передачи сообщения
    Стеганография
    Криптография
    Криптоанализ
4. ### - это процесс преобразования исходного (открытого) сообщения в шифрованное по определенным правилам, содержащимся в шифре

5. ### - это процесс преобразования шифрованного сообщения (шифртекста) в исходное (открытое) сообщение с помощью определенных правил, содержащихся в шифре
6. Способ преобразования информации с целью ее защиты от незаконных пользователей называется:
   - шифром
   - шифрованием
   - дешифрованием
7. Процесс получения защищенного сообщения (открытого текста) из шифрованного сообщения (шифртекста) без знания примененного шифра называется:
   - вскрытием шифра
   - шифрованием
   - дешифрованием
8. Сменный элемент шифра, применяемый для шифрования конкретных сообщений, называется:
   - ключом
   - шифром
   - ширфтекстом
9. Укажите способы преобразования при шифровании:
   - подстановка
   - перестановка
   - аналитическое преобразование
   - гаммирование
   - кодирование
10. Криптосистемой является:
    - семейство обратимых преобразований открытого текста в шифрованный;
    - семейство необратимых преобразований открытого текста в шифрованный;
    - средство аппаратной защиты данных;
    - система несанкционированного доступа к тексту
11. Что из перечисленного не входит в криптосистему:
    - полиморфик-генератор
    - алгоритм шифрования
    - набор ключей, используемых для шифрования
    - система управления ключами
12. ГОСТ 28147-89 является стандартом:
    - симметричного шифрования;
    - асимметричного шифрования;
    - гаммирования;
    - стеганографии
13. Алгоритм RSA является стандартом:
    - симметричного шифрования;
    - асимметричного шифрования;
    - гаммирования;
    - стеганографии
14. При асимметричном шифровании для шифрования и расшифровки используются:
    - два взаимосвязанных ключа;
    - один открытый ключ;
    - один закрытый ключ;
    - два открытых ключа
15. Реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа, предназначенный для защиты данного документа от подделки, и позволяющий идентифицировать владельца ключа,

а также установить отсутствие искажения информации в электронном документе, представляет собой:

электронную цифровую подпись;
закрытый ключ шифрования;
вирусную маску;
открытый ключ шифрования

16. Цифровая подпись не обеспечивает:
    контроль целостности документа
    конфиденциальность документа
    доказательное подтверждение авторства документа
    восстановление поврежденного документа
17. Укажите виды цифровой подписи:
    простая цифровая подпись
    усиленная цифровая подпись
    квалифицированная цифровая подпись
    неквалифицированная цифровая подпись
18. Алгоритмы шифрования бывают:
    многоядерные
    с использованием хэш-функций
    периодические
    рекурсивные
19. Алгоритмы шифрования бывают:
    апериодические
    асимметричные
    рекурсивные
20. Электронно-цифровая подпись устанавливает ??? информации:
    непротиворечивость
    разрешение
    противоречивость
    целостность
21. Цифровая подпись обеспечивает:
    невозможность отказа от авторства
    удаленный доступ к документу
    быструю пересылку документа
    защиту от изменений конфигурации ОС
22. Цифровая подпись обеспечивает:
    удостоверение источника документа
    быструю пересылку документа
    защиту от изменений трафика
    удаленный доступ к документу
23. Программные модули или аппаратные устройства, регистрирующие каждое нажатие клавиши на клавиатуре компьютера :
    скриншоты
    кейлоггеры
    браузеры
    брандмауэры
24. Для генерации ЭЦП может быть использован алгоритм:
    DES
    RSA
    AES
25. Какие из перечисленных алгоритмов относятся к симметричным?
    DES;

RSA;
ГОСТ 28147-89

26. Для контроля целостности передаваемых по сетям данных используется:
    электронная цифровая подпись;
    аутентификация данных;
    аудит событий;
    межсетевое экранирование
27. Что не является задачей криптосистемы:
    межсетевое экранирование;
    обеспечение конфиденциальности;
    обеспечение целостности данных;
    аутентификация данных и их источников
28. Что из перечисленного не является функцией управления криптографическими ключами:
    изучение;
    генерация;
    хранение;
    распределение
29. Программная или программно-аппаратная система, которая выполняет контроль информационных потоков, поступающих в информационную систему и/или выходящих из нее, и обеспечивает защиту информационной системы посредством фильтрации информации называется:
    межсетевым экраном;
    криптоалгоритмом;
    сервером удаленного доступа;
    криптосистемой
30. Электронно-цифровая подпись позволяет:
    удостовериться в истинности отправителя и целостности сообщения;
    восстанавливать поврежденные сообщения;
    пересылать сообщения по секретному каналу;
    зашифровать сообщение для сохранения его секретности
31. Криптосистемой является:
    семейство обратимых преобразований открытого текста в шифрованный;
    семейство необратимых преобразований открытого текста в шифрованный;
    средство аппаратной защиты данных;
    система несанкционированного доступа к тексту
32. ГОСТ 2814789 является стандартом:
    симметричного шифрования;
    асимметричного шифрования;
    гаммирования;
    стеганографии
33. Размер ключа в ГОСТ 28147-89:
    256 бит;
    64 бита;
    56 бит;
    128 бит
34. Размер ключа в стандарте DES:
    256 бит;
    64 бита;
    56 бит;
    128 бит

Раздел №8. Обеспечение безопасности систем, входящих в состав глобальных компьютерных сетей

1. ### - это устройство контроля доступа в сеть, предназначенное для блокировки всего трафика, за исключением разрешенных данных.
2. Функцией ??? является доставка трафика в пункт назначения в максимально короткие сроки:
   Межсетевого экрана;
   Маршрутизатора;
   Концентратора
3. Укажите типы межсетевых экранов:
   виртуальные межсетевые экраны;
   межсетевые экраны прикладного уровня;
   межсетевые экраны с пакетной фильтрацией;
   гибридные межсетевые экраны.
4. В межсетевом экране ??? каждому разрешаемому протоколу должен соответствовать свой собственный модуль доступа:
   прикладного уровня;
   с пакетной фильтрацией;
   гибридном;
   виртуальном.
5. Какой тип межсетевых экранов использует модули доступа для входящих подключений:
   виртуальные;
   прикладного уровня;
   с пакетной фильтрацией;
   гибридные.
6. В межсетевых экранах какого типа правила политики устанавливаются посредством использования фильтров пакетов:
   В виртуальных межсетевых экранах;
   В межсетевых экранах прикладного уровня;
   В межсетевые экраны с пакетной фильтрацией;
   В гибридных межсетевых экранах.
7. Укажите назначение системы обнаружения вторжений IDS :
   разграничение авторизованного входа и несанкционированного проникновения;
   доставка трафика в пункт назначения;
   блокировки всего трафика.
8. ??? служит для предотвращения доступа из внешней сети к ресурсам и компьютерам внутренней сети за счет выноса из локальной сети в особую зону всех сервисов, требующих доступа извне:
   Демилитаризованная зона;
   Система обнаружения вторжений;
   Межсетевой экран.
9. Укажите цели использования системы обнаружения вторжений:
   Обнаружение и предотвращение атак;
   Обнаружение нарушений политики безопасности;
   Принуждение к использованию политик безопасности;
   Просмотр зашифрованного трафика;
   Отслеживание определенных соединений и ведение журнала по учету трафика.
10. Укажите основные типы систем обнаружения вторжений:
    Узловые (HIDS);
    Сетевые IDS (NIDS);
    Периферийные IDS (PIDS).
11. Какого типа систем обнаружения вторжений (IDS) располагается на отдельном узле и отслеживает признаки атак на данный узел:
    Узловые (HIDS);

Сетевые IDS (NIDS);
Периферийные IDS (PIDS).

12. ??? систем обнаружения вторжений (IDS) находится на отдельной системе, отслеживающей сетевой трафик на наличие признаков атак, проводимых в подконтрольном сегменте сети:
Узловые (HIDS);
Сетевые IDS (NIDS);
Периферийные IDS (PIDS).

3.8. Контроль умений и навыков

Контроль умений и навыков осуществляется на лабораторных занятиях во время приема отчетов обучающихся о выполнении индивидуальных заданий в соответствии с планом проведения лабораторных занятий и в ходе опроса обучающихся при контроле выполнения ими индивидуальных заданий.

Оценка овладения навыками осуществляется через решение обучающимися следующих практических задач:

- определение целей защиты информации в организации;
- рассмотрение особенностей объекта защиты информации;
- определение угроз информационной безопасности;
- проведение анализа рисков информационной безопасности в организации;
- построение концепции информационной безопасности в организации;
- реализация защиты информации средствами ОС, MS Office, криптографии;
- реализация защиты информации средствами криптографии.

4. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности

4.1. Внутренние нормативные акты

Положение о текущем контроле успеваемости и промежуточной аттестации обучающихся П ВГАУ 1.1.01 – 2017;

Положение о фонде оценочных средств П ВГАУ 1.1.13 – 2016

4.2. Рекомендации по проведению текущего контроля

1.	Сроки проведения текущего контроля	На каждом лабораторном занятии
2.	Место и время проведения текущего контроля	В учебной аудитории в ходе лабораторного занятия
3.	Требования к техническому оснащению аудитории	В соответствии с ОПОП и рабочей программой
4.	Лицо, проводящее процедуру контроля	Преподаватель, ведущий лабораторные занятия
5.	Форма текущего контроля	Опрос, собеседование, тестирование
6.	Время для проведения текущего контроля	В течение занятия
7.	Возможность использования дополнительными материалами	Разрешается
8.	Лицо, обрабатывающее результаты	Преподаватель, ведущий лабораторные занятия
9.	Методы оценки результатов	Экспертный

10.	Предъявление результатов	Оценка выставляется в журнал, доводится до сведения обучающихся в течение занятия
11.	Апелляция результатов	В порядке, установленном внутренними нормативными актами