

Федеральное государственное бюджетное образовательное учреждение высшего образования «Тамбовский государственный университет имени Г.Р. Державина»
Институт математики, физики и информационных технологий
Кафедра математического моделирования и информационных технологий

УТВЕРЖДАЮ:
Директор института



Н. Л. Королева
«05» июля 2021 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине Б1.О.11 Введение в специальность

Направление подготовки/специальность: 10.05.05 - Безопасность информационных технологий в правоохранительной сфере

Профиль/направленность/специализация: Технологии защиты информации в правоохранительной сфере

Уровень высшего образования: специалитет

Квалификация: Специалист по защите информации

год набора: 2021

Автор программы:

Анурьева Мария Сергеевна

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.05 - Безопасность информационных технологий в правоохранительной сфере (уровень специалитета) (приказ Министерства образования и науки РФ от «26» ноября 2020 г. № 1461).

Рабочая программа принята на заседании Кафедры математического моделирования и информационных технологий «18» мая 2021 г. Протокол № 9

Рассмотрена и одобрена на заседании Ученого совета Института математики, физики и информационных технологий, Протокол от «05» июля 2021 г. № 5.

СОДЕРЖАНИЕ

| | |
|---------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 1. Цели и задачи дисциплины..... | 4 |
| 2. Место дисциплины в структуре ОП Специалиста..... | 5 |
| 3. Объем и содержание дисциплины..... | 5 |
| 4. Контроль знаний обучающихся и типовые оценочные средства..... | 12 |
| 5. Методические указания для обучающихся по освоению дисциплины (модуля)..... | 40 |
| 6. Учебно-методическое и информационное обеспечение дисциплины..... | 41 |
| 7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы..... | 42 |

1. Цели и задачи дисциплины

1.1 Цель дисциплины – формирование компетенций:

ОПК-9 Способен применять технологии получения, накопления, хранения, обработки, интерпретации и использования информации в ходе профессиональной деятельности

1.2 Типы задач профессиональной деятельности, к которым готовятся обучающиеся в рамках освоения дисциплины:

- аналитический
- организационно-управленческий
- эксплуатационный

1.3 Дисциплина ориентирована на подготовку обучающихся к профессиональной деятельности в сферах: 06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере), 12 Обеспечение безопасности (в сфере защиты информации), Сфера правоохранительной деятельности

1.4 В результате освоения дисциплины у обучающихся должны быть сформированы:

| Обобщенные трудовые функции / трудовые функции / трудовые или профессиональные действия (при наличии профстандарта) | Код и наименование компетенции ФГОС ВО, необходимой для формирования трудового или профессионального действия | Индикаторы достижения компетенций |
|---------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| | ОПК-9 Способен применять технологии получения, накопления, хранения, обработки, интерпретации и использования информации в ходе профессиональной деятельности | Применяет технологии получения, накопления, хранения, обработки, интерпретации и использования информации в ходе профессиональной деятельности |

1.5 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

ОПК-9 Способен применять технологии получения, накопления, хранения, обработки, интерпретации и использования информации в ходе профессиональной деятельности

| № п/п | Наименование дисциплин, определяющих междисциплинарные связи | Форма обучения | |
|-------|-------------------------------------------------------------------------|-----------------|---|
| | | Очная (семестр) | |
| | | 2 | 4 |
| 1 | Специальные информационные технологии в правоохранительной деятельности | | + |

| | | | |
|---|--------------------------------------------------------------------------------|---|--|
| 2 | Теория информационной безопасности и методология защиты информации | + | |
|---|--------------------------------------------------------------------------------|---|--|

2. Место дисциплины в структуре ОП специалитета:

Дисциплина «Введение в специальность» относится к обязательной части учебного плана ОП по направлению подготовки 10.05.05 - Безопасность информационных технологий в правоохранительной сфере.

Дисциплина «Введение в специальность» изучается в 1 семестре.

3. Объем и содержание дисциплины

3.1. Объем дисциплины: 3 з.е.

Очная: 3 з.е.

| Вид учебной работы | Очная (всего часов) |
|--------------------------------------|------------------------|
| Общая трудоёмкость дисциплины | 108 |
| Контактная работа | 32 |
| Лекции (Лекции) | 16 |
| Практические (Практ. раб.) | 16 |
| Самостоятельная работа (СР) | 40 |
| Экзамен | 36 |

3.2. Содержание курса:

| № темы | Название раздела/темы | Вид учебной работы, час. | | | Формы текущего контроля |
|-----------|-----------------------------------------------------------------------------------------|-----------------------------|--------------------|----|------------------------------------------------------------|
| | | Лек ции | Пра кт. раб. | СР | |
| | | О | О | О | |
| 1 семестр | | | | | |
| 1 | Карьерный навигатор по ИТ-специальностям | 2 | 2 | 4 | Собеседование; Практическое задание; Тестирование |
| 2 | История защиты информации. Криптографические и стеганографические методы | 2 | 2 | 4 | Собеседование; Практическое задание; Тестирование |
| 3 | Современные криптографические протоколы | 2 | 2 | 4 | Собеседование; Практическое задание; Тестирование |
| 4 | Информационная безопасность пользователя | 2 | 2 | 4 | Собеседование; Практическое задание; Тестирование |

| | | | | | |
|---|---------------------------------------------------------------------------|---|---|---|---------------------------------------------------------|
| 5 | Терминологические основы информационной безопасности | 2 | 2 | 6 | Собеседование; Практическое задание; Тестирование |
| 6 | Нормативно-правовое обеспечение информационной безопасности в РФ. | 2 | 2 | 6 | Собеседование; Практическое задание; Тестирование |
| 7 | Структура информационной безопасности, применяемая в общемировой практике | 2 | 2 | 8 | Реферат; Тестирование |
| 8 | Угрозы информационной безопасности | 2 | 2 | 4 | Собеседование; Практическое задание; Тестирование |

Тема 1. Карьерный навигатор по ИТ-специальностям (ОПК-9)

Лекция.

Лекция направлена на раскрытие темы какие ИТ-специальности существуют в современном мире, какие задачи стоят перед ИТ специалистами в компаниях, и как развивать ИТ-компетенции у своих работников, какие новые специальности формируются на стыке отраслевых специальностей с ИТ сферой, какие компетенции будут востребованы в ближайшем будущем. Раскрываются понятия сквозные технологии, которые включают в себя: Большие данные; Машинное обучение; Искусственный интеллект; Дополненная реальность; Виртуальная реальность; Робототехника; Блокчейн; Интернет вещей; 5 G.

Практическое занятие.

Практическая работа № 1. Исследование рынка трудоустройства специалистов по информационной безопасности

На основе открытых данных сайтов действующих вакансий проведите анализ рынка трудоустройства специалистов по информационной безопасности. Заполните таблицу по результатам анализа, где отразите найденную информацию: вакансия, регион, компания, заработная плата, требования к квалификации.

Отчет должен содержать:

1. Титульный лист
2. Содержание
3. Сводная таблица по результатам поиска
4. Список использованных источников

Задания для самостоятельной работы.

Цель самостоятельной работы – содействие оптимальному усвоению студентами учебного материала.

Задачи самостоятельной работы:

углубление и систематизация знаний;

развитие аналитических способностей умственной деятельности, умений работы с различной по объёму и виду информацией, учебной и научной литературой.

Задание:

Записать краткий конспект лекции.

Изучить базовую и дополнительную литературу по теме лекции

Ответить на вопросы для самоконтроля

Тема 2. История защиты информации. Криптографические и стеганографические методы (ОПК-9)

Лекция.

Понятия криптологии, криптографии, криптоанализа, ключ шифра. Первые шифры замены и перестановки (шифр сдвиг, шифр Цезаря). Шифр Виженера. Решетка Кардано. Стеганографические методы защиты информации. Становление математических и технических основ защиты информации в Новое время. Начало формирования научных приёмов защиты информации. Изобретение электромагнитного телеграфа и первых механических шифромашин. Семейство машин Энигма. Криптоанализ шифра Энигма. Изобретение совершенно секретного шифра («одноразовый шифроблокнот»), преимущества и проблемы его использования.

Практическое занятие.

Практическая работа 2.1 Шифрование с помощью системы Цезаря.

Зашифруйте сообщение «НАСТОЯЩИЙ ДРУГ С ТОБОЙ, КОГДА ТЫ НЕ ПРАВ. КОГДА ТЫ ПРАВ, ВСЯКИЙ БУДЕТ С ТОБОЙ» (Марк Твен), используя систему Цезаря со значением ключа соответствующим номеру вашего варианта по журналу учебной группы (например, номер по списку – 5; вариант – 5; ключ $K = 5$).

Отчет по практической работе должен включать: титульный лист, ход работы (шифрование текста личным ключом), ответы на вопросы.

Практическая работа 2.2 Шифрование с помощью шифра Виженера

Используя систему Виженера, зашифруйте сообщения по вариантам, приведенным в таблице 2.

Текст сообщения и ключевое слово должны соответствовать вашему варианту по журналу учебной группы (например, если номер по списку 3, значит вариант – 3).

Отчет по практической работе должен включать: титульный лист, ход работы (шифрование текста личным ключом), ответы на вопросы.

Задания для самостоятельной работы.

Цель самостоятельной работы – содействие оптимальному усвоению студентами учебного материала.

Задачи самостоятельной работы:

углубление и систематизация знаний;

развитие аналитических способностей умственной деятельности, умений работы с различной по объёму и виду информацией, учебной и научной литературой.

Задание:

Записать краткий конспект лекции.

Изучить базовую и дополнительную литературу по теме лекции

Ответить на вопросы для самоконтроля

Тема 3. Современные криптографические протоколы (ОПК-9)

Лекция.

Понятие криптографического протокола. Ключи. Симметричные методы шифрования (шифрование с закрытым ключом): технологии, стойкость, преимущества и недостатки. Асимметричные методы шифрования (шифрование с открытым ключом): технологии, стойкость, преимущества и недостатки. Атака "человек посередине". Цифровая подпись. Сертификаты и удостоверяющие центры.

Практическое занятие.

Практическая работа 3.1. Сравнение данных с помощью хэш-функции.

Важно понимать, были ли данные повреждены или была совершена попытка их фальсификации. Для определения того, были ли данные изменены или остались такими же, можно использовать программу хэширования. Программа хэширования выполняет преобразование данных или файла используя хэш-функцию, которая выдает некое значение (обычно значительно короче, чем сами исходные данные). Существует множество разных хэш-функций, одни очень простые, другие, напротив, очень сложные. Если одна и та же хэш-функция выполняется для преобразования одних и тех же данных, то значение, которое будет получено, будет всегда одинаково. Если данные были каким-то образом изменены, то полученное значение хэш-функцией будет отличаться.

Практическая работа 3.2. Стеганографические методы защиты информации (сокрытие текстового файла в графическом)

Необходимо знакомиться с теоретическим материалом. Произвести установку программного продукта Masker; спрятать текстовый файл в изображении, выбрав алгоритм шифрования пароля; отправить зашифрованное сообщение по электронной почте; извлечь текстовый файл из изображения; удалить извлечённый текстовый файл, без возможности для восстановления.

Задания для самостоятельной работы.

Цель самостоятельной работы – содействие оптимальному усвоению студентами учебного материала.

Задачи самостоятельной работы:

углубление и систематизация знаний;

развитие аналитических способностей умственной деятельности, умений работы с различной по объёму и виду информацией, учебной и научной литературой.

Задание:

Записать краткий конспект лекции.

Изучить базовую и дополнительную литературу по теме лекции

Ответить на вопросы для самоконтроля

Тема 4. Информационная безопасность пользователя (ОПК-9)

Лекция.

Фишинг. Основные варианты фишинга. Способы фишинга. Тайпсвотинг. Троянский конь. Квид про Кво. Претекстинг. «Дорожное яблоко». Сбор информации из открытых источников. Обратная социальная инженерия. Вредоносное ПО. Способы защиты информации от вредоносного ПО. Стойкость паролей.

Практическое занятие.

Практическая работа 4. 1 «Сможете ли вы распознать фишинговую атаку»

Тест «Сможете ли вы распознать фишинговую атаку»

<https://phishingquiz.withgoogle.com/>

Отчет по работе - скриншот с результатами теста

Задания для самостоятельной работы.

Цель самостоятельной работы – содействие оптимальному усвоению студентами учебного материала.

Задачи самостоятельной работы:

углубление и систематизация знаний;

развитие аналитических способностей умственной деятельности, умений работы с различной по объёму и виду информацией, учебной и научной литературой.

Задание:

Записать краткий конспект лекции.

Изучить базовую и дополнительную литературу по теме лекции

Ответить на вопросы для самоконтроля

Тема 5. Терминологические основы информационной безопасности (ОПК-9)

Лекция.

Понятие информации, информатизации, информационных систем и смежных с ними: информационная безопасность, информационная война, информационная агрессия, информационное оружие, информационные процессы, информационная система, информационная сфера. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации, тайна, средства защиты информации, угрозы - определения, сопоставление.

Практическое занятие.

Практическая работа №5

«Терминология в области информационной безопасности»

Задание. 1. В сети Интернет найдите определения нижеперечисленным терминам, обращая внимание на степень достоверности источника (возможно указать несколько разных определений для одного и того же термина). Для каждого определения необходимо обозначить источник.

Задание 2. Самостоятельно попытайтесь объединить нижеперечисленные понятия в группы по определенным признакам, которые вам покажутся наиболее важными.

Задание 3. Понятия, выделенные жирным шрифтом необходимо выучить наизусть.

1. Информационная безопасность
2. Защита информации
3. Конфиденциальность
4. Целостность
5. Доступность
6. Угроза безопасности информации
7. Источник угрозы
8. Объект защиты информации
9. Уязвимость
10. Идентификация
11. Аутентификация
12. Организационные меры по защите информации
13. Технические меры по защите информации
14. Программно-аппаратные меры по защите информации
15. Криптографическая защита информации
16. Правовая защита информации
17. Способ защиты информации
18. Защита информации от несанкционированного воздействия
19. Политика безопасности
20. Носитель защищаемой информации
21. Средство защиты информации
22. Лицензирование в области защиты информации
23. Сертификация на соответствие требованиям по безопасности информации
24. Аудит и аттестация объектов информатизации
25. Анализ информационного риска
26. Требование по защите информации
27. Эффективность защиты информации
28. Атака
29. Злоумышленник
30. Идентификатор
31. Пароль
32. Ключ

33. Учетная запись пользователя
34. Снифер
35. Спуфер
36. Сканирование портов
37. Отказ от обслуживания
38. Утечка
39. Разглашение.
40. Пен-тест

Задания для самостоятельной работы.

Цель самостоятельной работы – содействие оптимальному усвоению студентами учебного материала.

Задачи самостоятельной работы:

углубление и систематизация знаний;

развитие аналитических способностей умственной деятельности, умений работы с различной по объёму и виду информацией, учебной и научной литературой.

Задание:

Записать краткий конспект лекции.

Изучить базовую и дополнительную литературу по теме лекции

Ответить на вопросы для самоконтроля

Тема 6. Нормативно-правовое обеспечение информационной безопасности в РФ. (ОПК-9)

Лекция.

В состав законодательства по обеспечению информационной безопасности включаются федеральные законы, подзаконные нормативные правовые акты федеральных органов исполнительной власти, законы и подзаконные нормативные правовые акты субъектов Российской Федерации.

Практическое занятие.

Практическая работа 6. Нормативные правовые акты в области информационной безопасности РФ

Цель: ознакомиться с нормативными правовыми актами в области информационной безопасности, проанализировать систему действующих правовых актов РФ в области информационной безопасности, формировать устойчивые навыки самостоятельной работы.

Практическая работа выполняется с использованием сети Интернет, (поисковая работа, анализ источников).

Аналитическая записка должна содержать иерархическую структуру исследованных правовых актов, сферу действия отдельных групп документов, соотношение и согласование групп правовых актов.

Содержание отчета: Тема, цель, перечень нормативно-правовых актов с полными реквизитами, ответы на контрольные вопросы, аналитическая записка.

Задания для самостоятельной работы.

Цель самостоятельной работы – содействие оптимальному усвоению студентами учебного материала.

Задачи самостоятельной работы:

углубление и систематизация знаний;

развитие аналитических способностей умственной деятельности, умений работы с различной по объёму и виду информацией, учебной и научной литературой.

Задание:

Записать краткий конспект лекции.

Изучить базовую и дополнительную литературу по теме лекции

Ответить на вопросы для самоконтроля

Тема 7. Структура информационной безопасности, применяемая в общемировой практике (ОПК-9)

Лекция.

Правовая защита информации. Организационная защита информации. Техническая или инженерно-техническая защита. Программно-аппаратная защита. Математические или криптографические методы. Психологические виды защиты информации. Морально-этические виды защиты информации. Страховая защита информации.

Практическое занятие.

Подготовка реферата и доклада по выбранной теме

Подготовка реферата и доклада по выбранной теме с использованием материалов баз научных статей (<https://elibrary.ru>, <https://cyberleninka.ru/>).

Цель реферата – приобретение студентами навыков самостоятельной работы по подбору, изучению, анализу и обобщению литературных источников. Объем реферата составляет 15-20 страниц.

Критерии оценки реферата

Соответствие содержания теме.

Правильность и полнота использования источников.

Соответствие оформления реферата стандартам.

Задания для самостоятельной работы.

Цель самостоятельной работы – содействие оптимальному усвоению студентами учебного материала.

Задачи самостоятельной работы:

углубление и систематизация знаний;

развитие аналитических способностей умственной деятельности, умений работы с различной по объёму и виду информацией, учебной и научной литературой.

Задание:

Записать краткий конспект лекции.

Изучить базовую и дополнительную литературу по теме лекции

Ответить на вопросы для самоконтроля

Тема 8. Угрозы информационной безопасности (ОПК-9)

Лекция.

Понятие угрозы. Виды угроз. 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. Характер происхождения угроз: умышленные факторы, естественные факторы. Источники угроз. Предпосылки появления угроз: объективные, субъективные

Практическое занятие.

Практическая работа 8 . Kaspersky Internet Security

Цель работы. Рассмотреть средства защиты, интегрированные в Kaspersky Internet Security_12.0.0.374ru_ru и настроить приложения

Ответить на вопросы, выполнить задания.

Отчет должен включать титульный лист, ход работы (с включением скриншотов и описанием действий), ответы на вопросы.

Prakticheskaya_rabota_Kaspersky_Internet_Security.pdf

Prakticheskaya_rabota_Kaspersky_Internet_Security.pdf

Задания для самостоятельной работы.

Цель самостоятельной работы – содействие оптимальному усвоению студентами учебного материала.

Задачи самостоятельной работы:

углубление и систематизация знаний;

развитие аналитических способностей умственной деятельности, умений работы с различной по объёму и виду информацией, учебной и научной литературой.

Задание:

Записать краткий конспект лекции.

Изучить базовую и дополнительную литературу по теме лекции

Ответить на вопросы для самоконтроля

4. Контроль знаний обучающихся и типовые оценочные средства

4.1. Распределение баллов:

1 семестр

- текущий контроль – 67 баллов
- контрольные срезы – 2 среза: 2 балла, 1 балл
- премиальные баллы – 10 баллов
- ответ на экзамене: не более 30 баллов

Распределение баллов по заданиям:

| № те мы | Название темы / вид учебной работы | Формы текущего контроля / срезы | Мах. кол-во баллов | Методика проведения занятия и оценки |
|---------|------------------------------------------|---------------------------------|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Карьерный навигатор по ИТ-специальностям | Собеседование | 1 | <p>Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определённому разделу, теме, проблеме и т.п. Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения поставленной учебной задачи; - своевременность и эффективность использования наглядных пособий и технических средств при ответе; - использование дополнительного материала; - рациональность использования времени, отведенного на задание. <p>1 балл - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается</p> |

| | | | | |
|----|--------------------------------------------------------------------------|---------------------------------|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | Практическое задание | 4 | <p>Практические задания выполняются по тематике практических занятий.</p> <p>3 балла – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию</p> <p>2 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы</p> <p>1 балл - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенные ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы</p> |
| | | Тестирование | 3 | <p>Оценка теста по текущему разделу или теме дисциплины</p> <p>3 балла – студент правильно отвечает на 50-100% вопросов в тесте.</p> <p>1 балла - студент правильно отвечает на 25-50% вопросов в тесте.</p> |
| | | | | |
| 2. | История защиты информации. Криптографические и стеганографические методы | Собеседование(контрольный срез) | 2 | <p>Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения поставленной учебной задачи; - своевременность и эффективность использования наглядных пособий и технических средств при ответе; - использование дополнительного материала; - рациональность использования времени, отведенного на задание. <p>1 балл – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается</p> |

| | | | | |
|----|-----------------------------------------|----------------------|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | Практическое задание | 4 | <p>Практические задания выполняются по тематике практических занятий.</p> <p>3 балла – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию</p> <p>2 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы</p> <p>1 балл - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенные ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы</p> |
| | | Тестирование | 3 | <p>Оценка теста по текущему разделу или теме дисциплины</p> <p>3 балла – студент правильно отвечает на 50-100% вопросов в тесте.</p> <p>1 балла - студент правильно отвечает на 25-50% вопросов в тесте.</p> |
| | | Собеседование | 1 | <p>Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения поставленной учебной задачи; - своевременность и эффективность использования наглядных пособий и технических средств при ответе; - использование дополнительного материала; - рациональность использования времени, отведенного на задание. <p>1 балл - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается</p> |
| 3. | Современные криптографические протоколы | | | |

| | | | | |
|----|------------------------------------------|----------------------|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | Практическое задание | 4 | <p>Практические задания выполняются по тематике практических занятий.</p> <p>3 балла – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию</p> <p>2 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы</p> <p>1 балл - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенные ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы</p> |
| | | Тестирование | 3 | <p>Оценка теста по текущему разделу или теме дисциплины</p> <p>3 балла – студент правильно отвечает на 50-100% вопросов в тесте.</p> <p>1 балла - студент правильно отвечает на 25-50% вопросов в тесте.</p> |
| | | Собеседование | 1 | <p>Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения поставленной учебной задачи; - своевременность и эффективность использования наглядных пособий и технических средств при ответе; - использование дополнительного материала; - рациональность использования времени, отведенного на задание. <p>2 балла – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы</p> <p>1 балл - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается</p> |
| 4. | Информационная безопасность пользователя | | | |

| | | | | |
|----|------------------------------------------------------|----------------------|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | Практическое задание | 4 | <p>Практические задания выполняются по тематике практических занятий.</p> <p>3 балла – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию</p> <p>2 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы</p> <p>1 балл - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенные ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы</p> |
| | | Тестирование | 3 | <p>Оценка теста по текущему разделу или теме дисциплины</p> <p>3 балла – студент правильно отвечает на 50-100% вопросов в тесте.</p> <p>1 балла - студент правильно отвечает на 25-50% вопросов в тесте.</p> |
| | | Собеседование | 1 | <p>Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения поставленной учебной задачи; - своевременность и эффективность использования наглядных пособий и технических средств при ответе; - использование дополнительного материала; - рациональность использования времени, отведенного на задание. <p>2 балла – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы</p> <p>1 балл - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается</p> |
| 5. | Терминологические основы информационной безопасности | | | |

| | | | | |
|----|-------------------------------------------------------------------|---------------------------------|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | Практическое задание | 4 | <p>Практические задания выполняются по тематике практических занятий.</p> <p>3 балла – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию</p> <p>2 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы</p> <p>1 балл - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенные ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы</p> |
| | | Тестирование | 3 | <p>Оценка теста по текущему разделу или теме дисциплины</p> <p>3 балла – студент правильно отвечает на 50-100% вопросов в тесте.</p> <p>1 балла - студент правильно отвечает на 25-50% вопросов в тесте.</p> |
| | | | | |
| 6. | Нормативно-правовое обеспечение информационной безопасности в РФ. | Собеседование(контрольный срез) | 1 | <p>Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения поставленной учебной задачи; - своевременность и эффективность использования наглядных пособий и технических средств при ответе; - использование дополнительного материала; - рациональность использования времени, отведенного на задание. <p>2 балла – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы</p> <p>1 балл - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается</p> |

| | | | | |
|----|---------------------------------------------------------------------------|----------------------|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | Практическое задание | 4 | <p>Практические задания выполняются по тематике практических занятий.</p> <p>3 балла – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию</p> <p>2 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы</p> <p>1 балл - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенные ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы</p> |
| | | Тестирование | 3 | <p>Оценка теста по текущему разделу или теме дисциплины</p> <p>3 балла – студент правильно отвечает на 50-100% вопросов в тесте.</p> <p>1 балла - студент правильно отвечает на 25-50% вопросов в тесте.</p> |
| | | Реферат | 10 | <p>10 баллов – реферат выполнен обучающимся самостоятельно, в полном объеме, с соблюдением необходимых технических параметров; стиль изложения отвечает специфике жанра научной работы; во введении логично, объективно и аргументировано характеризуется научная проблема; содержание реферата включает самостоятельное исследование, а заключение содержат выводы, логично вытекающие из содержания основной части; список литературы оформлен в соответствии с правилами ГОСТа</p> <p>8 балла – во введение четко сформулированы основные позиции реферата, а содержание соответствует теме реферата; в содержании реферата логично, связно, но недостаточно полно излагается теоретическая или практическая часть; заключение содержит выводы, логично вытекающие из содержания основной части; стиль изложения соответствует специфике жанра научной работы; в оформлении списка литературы встречаются незначительные погрешности</p> <p>1-2 балла – текст реферата представляет несамостоятельное (компиляция; плагиат) научное исследование; реферат написан с несоблюдением технических и научных требований</p> |
| 7. | Структура информационной безопасности, применяемая в общемировой практике | Тестирование | 3 | <p>Оценка теста по текущему разделу или теме дисциплины</p> <p>3 балла – студент правильно отвечает на 50-100% вопросов в тесте.</p> <p>1 балла - студент правильно отвечает на 25-50% вопросов в тесте.</p> |

| | | | | |
|----|----------------------------------------------|-----------------------------|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8. | Угрозы информационн ой безопасности | Собеседо вание | 1 | <p>Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения поставленной учебной задачи; - своевременность и эффективность использования наглядных пособий и технических средств при ответе; - использование дополнительного материала; - рациональность использования времени, отведенного на задание. <p>2 балла – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы</p> <p>1 балл - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается</p> |
| | | Практиче ское задание | 4 | <p>Практические задания выполняются по тематике практических занятий.</p> <p>3 балла – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию</p> <p>2 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы</p> <p>1 балл - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы</p> |
| | | Тестиров ание | 3 | <p>Оценка теста по текущему разделу или теме дисциплины</p> <p>3 балла – студент правильно отвечает на 50-100% вопросов в тесте.</p> <p>1 балла - студент правильно отвечает на 25-50% вопросов в тесте.</p> |
| 9. | Премиальные баллы | | 10 | <p>Дополнительные премиальные баллы могут быть начислены:</p> <ul style="list-style-type: none"> - постоянная активность во время практических занятий – 10 баллов |

| | | | |
|-----|-------------------|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10. | Ответ на экзамене | 30 | 25-30 баллов – студент раскрыл основные вопросы и задания билета на оценку «отлично». 18-30 баллов – студент раскрыл основные вопросы и задания билета на оценку «хорошо», 10-17 баллов – студент раскрыл основные вопросы и задания билета на оценку «удовлетворительно» |
| 11. | Итого за семестр | 100 | |

Итоговая оценка по экзамену выставляется в 100-балльной шкале и в традиционной четырехбалльной шкале. Перевод 100-балльной рейтинговой оценки по дисциплине в традиционную четырехбалльную осуществляется следующим образом:

| 100-балльная система | Традиционная система |
|----------------------|----------------------|
| 85 - 100 баллов | Отлично |
| 70 - 84 баллов | Хорошо |
| 50 - 69 баллов | Удовлетворительно |
| Менее 50 | Неудовлетворительно |

4.2 Типовые оценочные средства текущего контроля

Практическое задание

Тема 1. Карьерный навигатор по ИТ-специальностям

Практическая работа № 1. Исследование рынка трудоустройства специалистов по информационной безопасности

На основе открытых данных сайтов действующих вакансий проведите анализ рынка трудоустройства специалистов по информационной безопасности. Заполните таблицу по результатам анализа, где отразите найденную информацию: вакансия, регион, компания, заработная плата, требования к квалификации.

Отчет должен содержать:

1. Титульный лист
2. Содержание
3. Сводная таблица по результатам поиска
4. Список использованных источников

Тема 2. История защиты информации. Криптографические и стеганографические методы

Практическая работа 2.1 Шифрование с помощью системы Цезаря.

Зашифруйте сообщение «НАСТОЯЩИЙ ДРУГ С ТОБОЙ, КОГДА ТЫ НЕ ПРАВ. КОГДА ТЫ ПРАВ, ВСЯКИЙ БУДЕТ С ТОБОЙ» (Марк Твен), используя систему Цезаря со значением ключа соответствующим номеру вашего варианта по журналу учебной группы (например, номер по списку – 5; вариант – 5; ключ $K = 5$).

Отчет по практической работе должен включать: титульный лист, ход работы (шифрование текста личным ключом), ответы на вопросы.

Практическая работа 2.2 Шифрование с помощью шифра Виженера

Используя систему Виженера, зашифруйте сообщения по вариантам, приведенным в таблице 2. Текст сообщения и ключевое слово должны соответствовать вашему варианту по журналу учебной группы (например, если номер по списку 3, значит вариант – 3).

Отчет по практической работе должен включать: титульный лист, ход работы (шифрование текста личным ключом), ответы на вопросы.

Тема 3. Современные криптографические протоколы

Практическая работа 3.1. Сравнение данных с помощью хэш-функции.

Важно понимать, были ли данные повреждены или была совершена попытка их фальсификации. Для определения того, были ли данные изменены или остались такими же, можно использовать программу хэширования. Программа хэширования выполняет преобразование данных или файла используя хэш-функцию, которая выдает некое значение (обычно значительно короче, чем сами исходные данные). Существует множество разных хэш-функций, одни очень простые, другие, напротив, очень сложные. Если одна и та же хэш-функция выполняется для преобразования одних и тех же данных, то значение, которое будет получено, будет всегда одинаково. Если данные были каким-то образом изменены, то полученное значение хэш-функцией будет отличаться.

Практическая работа 3.2. Стеганографические методы защиты информации (сокрытие текстового файла в графическом)

Необходимо знакомиться с теоретическим материалом. Произвести установку программного продукта Masker; спрятать текстовый файл в изображении, выбрав алгоритм шифрования пароля; отправить зашифрованное сообщение по электронной почте; извлечь текстовый файл из изображения; удалить извлечённый текстовый файл, без возможности для восстановления.

Тема 4. Информационная безопасность пользователя

Практическая работа 4. 1 «Сможете ли вы распознать фишинговую атаку»

Тест «Сможете ли вы распознать фишинговую атаку»

<https://phishingquiz.withgoogle.com/>

Отчет по работе - скриншот с результатами теста

Тема 5. Терминологические основы информационной безопасности

Практическая работа №5

«Терминология в области информационной безопасности»

Задание. 1. В сети Интернет найдите определения нижеперечисленным терминам, обращая внимание на степень достоверности источника (возможно указать несколько разных определений для одного и того же термина). Для каждого определения необходимо обозначить источник.

Задание 2. Самостоятельно попытайтесь объединить нижеперечисленные понятия в группы по определенным признакам, которые вам покажутся наиболее важными.

Задание 3. Понятия, выделенные жирным шрифтом необходимо выучить наизусть.

1. Информационная безопасность
2. Защита информации
3. Конфиденциальность
4. Целостность
5. Доступность
6. Угроза безопасности информации
7. Источник угрозы
8. Объект защиты информации
9. Уязвимость
10. Идентификация
11. Аутентификация
12. Организационные меры по защите информации
13. Технические меры по защите информации
14. Программно-аппаратные меры по защите информации
15. Криптографическая защита информации
16. Правовая защита информации
17. Способ защиты информации
18. Защита информации от несанкционированного воздействия
19. Политика безопасности

20. Носитель защищаемой информации
21. Средство защиты информации
22. Лицензирование в области защиты информации
23. Сертификация на соответствие требованиям по безопасности информации
24. Аудит и аттестация объектов информатизации
25. Анализ информационного риска
26. Требование по защите информации
27. Эффективность защиты информации
28. Атака
29. Злоумышленник
30. Идентификатор
31. Пароль
32. Ключ
33. Учетная запись пользователя
34. Снифер
35. Спуфер
36. Сканирование портов
37. Отказ от обслуживания
38. Утечка
39. Разглашение.
40. Пен-тест

Тема 6. Нормативно-правовое обеспечение информационной безопасности в РФ.

Практическая работа 6. Нормативные правовые акты в области информационной безопасности РФ

Цель: ознакомиться с нормативными правовыми актами в области информационной безопасности, проанализировать систему действующих правовых актов РФ в области информационной безопасности, формировать устойчивые навыки самостоятельной работы.

Практическая работа выполняется с использованием сети Интернет, (поисковая работа, анализ источников).

Аналитическая записка должна содержать иерархическую структуру исследованных правовых актов, сферу действия отдельных групп документов, соотношение и согласование групп правовых актов.

Содержание отчета: Тема, цель, перечень нормативно-правовых актов с полными реквизитами, ответы на контрольные вопросы, аналитическая записка.

Тема 8. Угрозы информационной безопасности

Практическая работа 8 . Kaspersky Internet Security

Цель работы. Рассмотреть средства защиты, интегрированные в Kaspersky Internet Security_12.0.0.374ru_ru и настроить приложения

Ответить на вопросы, выполнить задания.

Отчет должен включать титульный лист, ход работы (с включением скриншотов и описанием действий), ответы на вопросы.

Prakticheskaya_rabota_Kaspersky_Internet_Security.pdf

Prakticheskaya_rabota_Kaspersky_Internet_Security.pdf

Реферат

Тема 7. Структура информационной безопасности, применяемая в общемировой практике

1. - Двадцать первый век и проблемы информационной безопасности.
2. - Современные методы антивирусной защиты информации.
3. - Программные средства современных систем безопасности в информационных системах.

4. - Защита данных в сети Интернет.
5. - Личная информационная безопасность пользователя
6. - Информационная безопасность в бизнесе.
7. - Сертификация, лицензирование, сертификация и аттестация в области информационной безопасности.
8. - Служебная тайна. Коммерческая тайна. Государственная тайна.
9. - Экономика и правовые основы рынка интеллектуальной собственности.
10. - Экономическая информационная безопасность.
11. - Стандарты шифрования данных.
12. - Алгоритм шифрования данных IDEA.
13. - Блочные и поточные шифры
14. - Закон РФ об электронной подписи.
15. - Управление криптографическими ключами: генерация, хранение, распределение ключей.
16. Риск работы на персональном компьютере. Планирование безопасной работы на персональном компьютере.
17. Обеспечение информационной безопасности Российской Федерации
18. Безопасность работы в Интернет с использованием браузера.
19. Защита информации для электронной коммерции в Интернет
20. Стойкость алгоритмов шифрования. Типы алгоритмов шифрования. Примеры криптографических алгоритмов.
21. Противодействие несанкционированному межсетевому доступу. Использование межсетевых экранов (Firewall).
22. Особенности криптографического и стеганографического преобразования информации.
23. Защита офисных документов.
24. Общие подходы к построению парольных систем. Выбор паролей. Хранение паролей. Передача пароля по сети.
25. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Компьютерные преступления.
26. Обзор состояния систем защиты информации в РФ в ведущих зарубежных странах.
27. Организационное обеспечение информационной безопасности.
28. Инженерно-техническое обеспечение информационной безопасности.
29. Программно-аппаратное обеспечение информационной безопасности.
30. Правовое обеспечение информационной безопасности.

Собеседование

Тема 1. Карьерный навигатор по ИТ-специальностям

Ответить на вопросы для самоконтроля:

1. Перечислите основные профессиональные треки в ИТ.
2. По каким признакам можно классифицировать специалистов, занимающихся разработкой ПО?
3. Чем занимаются специалисты DevOps?
4. Сколько бывает линий поддержки при сопровождении пользователей? Какие функции выполняют специалисты по каждой линии?
5. Какие варианты деятельности есть в треке «Робототехника»?
6. Что такое джуниор-разработчик, мидл-разработчик и синьор-разработчик?
7. Охарактеризуйте направление деятельности QA-engineer.
8. Чем отличается UX-тестирование от UI-тестирования?
9. Какие виды роботов бывают?
10. Что входит в сферу деятельности технического писателя?
11. Есть ли отличие бизнес-аналитика от системного аналитика? Если да, то в чём?

12. Что входит в круг обязанностей проектного менеджера?

Тема 2. История защиты информации. Криптографические и стеганографические методы

Ответить на вопросы для самоконтроля:

1. В чем особенность шифров простой замены?
2. Чем отличаются система шифрования Цезаря и аффинная система подстановок Цезаря?
3. Какие требования предъявляются к выбору ключей для аффинной системы подстановок Цезаря?
4. Чем шифры простой замены отличаются от шифров сложной замены?
5. Какой ключ используется в системе Вижинера?
6. В чем заключается алгоритм шифрования текста с использованием системы Вижинера?
7. В чем заключались преимущества шифровальной машины Энигма?
8. Какие "уязвимости" шифровальной машины Энигма были использованы командой Алана Тьюринга?
9. Перечислите необходимые условия для абсолютно стойкого шифра.
10. В чем заключаются преимущества и недостатки одноразового шифроблокнота?
11. Чем отличаются понятия криптологии, криптографии, криптоанализа?
12. Что такое ключ шифра? Приведите примеры шифров с одним и двумя ключами.
13. В чем отличие шифра замены от шифра перестановки?

Тема 3. Современные криптографические протоколы

Ответить на вопросы для самоконтроля:

1. Что такое открытый ключ?
2. Чем симметричное шифрование отличается от асимметричного?
4. Что такое закрытый ключ?
5. Что такое электронная подпись?
6. Какими нормативно-правовыми документами устанавливаются основные действия с электронной подписью в России?
7. Достоинства и недостатки симметричного шифрования.
8. Достоинства и недостатки асимметричного шифрования.
9. Какой вид шифрования называют коммерческим? Почему?
10. Назовите области применения хэш-функций.
11. Применяют ли хэш-функции для шифрования сообщений? Объясните свой ответ.

Тема 4. Информационная безопасность пользователя

Ответить на вопросы для самоконтроля:

1. Что относится к фишинговым атакам?
2. Какие виды фишинговых атак вы знаете? Опишите их.
3. На какие виды делятся вредоносные программы?
4. Приведите пример методов социальной инженерии.
5. Что такое компьютерный вирус? В чем его главное отличие от других вредоносных программ?
6. Что такое сетевой червь?
7. Почему необходимо своевременно обновление ПО?
8. Объясните, как повышается стойкости пароли при увеличении количества символов и использовании дополнительных символов?

Тема 5. Терминологические основы информационной безопасности

Ответить на вопросы для самоконтроля:

1. Приведите примеры возможных подходов к классификации угроз безопасности информации.
2. В чем состоит суть системной классификации угроз?

3. По каким параметрам проводится системная классификация угроз?
4. Какие параметры автоматизированной системы, информации и ситуации защиты могут быть использованы для определения вероятности нарушения защищенности информации?
5. В чем заключается суть базового, обобщенного и общего показателей уязвимости информации?
6. Какие показатели используются для характеристики наиболее неблагоприятных ситуаций защиты?
7. Что вы можете сказать о формировании множества угроз безопасности информации?
8. Дайте определение информационной безопасности и защиты информации.

Тема 6. Нормативно-правовое обеспечение информационной безопасности в РФ.

1. Какой документ из перечня является высшим в иерархии правовых актов?
2. В составленном перечне отметьте правовые акты, регламентирующие технические условия
3. В составленном перечне отметьте правовые акты, регламентирующие организационные условия
4. Какие документы из представленного перечня являются следствием ассоциирования правовых актов РФ с международным законодательством

Тема 8. Угрозы информационной безопасности

1. Приведите примеры возможных подходов к классификации угроз безопасности информации.
2. В чем состоит суть системной классификации угроз?
3. По каким параметрам проводится системная классификация угроз?
4. Какие параметры автоматизированной системы, информации и ситуации защиты могут быть использованы для определения вероятности нарушения защищенности информации?
5. В чем заключается суть базового, обобщенного и общего показателей уязвимости информации?
6. Какие показатели используются для характеристики наиболее неблагоприятных ситуаций защиты?
7. Что вы можете сказать о формировании множества угроз безопасности информации?
8. Какие методы могут быть использованы для первоначального формирования возможно более полного множества угроз безопасности информации?

Тестирование

Тема 1. Карьерный навигатор по ИТ-специальностям

1. В РФ установлены _____ степени(-ей) дипломов о высшем образовании.

• три

2. Модель человеческого поведения, которая задана должностной позицией, т. е. набором функций, стереотипов поведения, средств самоподачи, которых ждет общество от носителя этой должностной позиции в деловом взаимодействии, называется:

• должностной ролью

3. _____ считал, что «налог есть такая форма доходов государства, когда эти доходы, получаемые с имущества граждан, являются их односторонней жертвой, без получения ими какого-либо эквивалента».

• Я. Таргулов

4. Документ учебного планирования, содержащий названия учебных дисциплин, время, отводимое на их изучение, распределение их по семестрам, — это учебный (ая) ...

• план

5. Оценка эффективности лекций в СГА проводилась по тестам

• Н. А. Аминова

Тема 2. История защиты информации. Криптографические и стеганографические методы

1 «Маски» вирусов используются

- + для поиска известных вирусов
- для поиска неизвестных вирусов
- для уничтожения известных вирусов
- для размножения вирусов
- для создания известных вирусов

2 IP-адрес имеет длину

- + 4 байта
- 8 байт
- 1 бит
- 8 бит
- 16 байт

3 Security updates (обновления безопасности) необходимы

- + для устранения обнаруженных недочетов в установленном ПО в операционных системах, установки патчей для предотвращения возможности эксплуатации уязвимостей, для поддержания внутренней самозащиты программ
- для поддержания внутренней самозащиты программ
- для обогащения вендоров, т.к. за дополнительные данные нужно платить
- для обновления внутренних модулей программ, чтобы приложения работали быстрее
- для облегчения работы с программами и улучшения восприятия интерфейса

4 Алгоритм DES использует длину блока:

- + 64 бит
- 256 бит
- 128 бит
- 8 бит
- 16 бит

5 Алгоритм DES использует длину ключа

- + 56 бит
- 256 бит
- 128 бит
- 8 бит
- 16 бит

6 Алгоритм Диффи-Хеллмана используется для

- + открытого распределения ключей
- вычисления хэш-функции
- генерации простых чисел
- генерации случайных чисел
- безопасного хранения ключей

7 Алгоритм Диффи-Хеллмана позволяет

- + использовать незащищенный от прослушивания, но защищенный от подмены, канал связи
- генерировать новые простые числа
- вычислить хэш функцию
- генерировать случайные числа
- безопасно хранить ключи

8 Алгоритм шифрования SHA предназначен для использования совместно с алгоритмом цифровой подписи

- + DSA
- DOS
- DES
- EGS
- RSA

Тема 3. Современные криптографические протоколы

1. Что является целью криптоанализа?

- A. Определение стойкости алгоритма
- B. Увеличение количества функций замещения в криптографическом алгоритме
- C. Уменьшение количества функций подстановки в криптографическом алгоритме
- D. Определение использованных перестановок

2. Частота применения брутфорс-атак возросла, поскольку:

- A. Возросло используемое в алгоритмах количество перестановок и замещений
- B. Алгоритмы по мере повышения стойкости становились менее сложными и более подверженными атакам
- C. Мощность и скорость работы процессоров возросла
- D. Длина ключа со временем уменьшилась

3. Что из перечисленного ниже не является свойством или характеристикой односторонней функции хэширования?

- A. Она преобразует сообщение произвольной длины в значение фиксированной длины
- B. Имея значение дайджеста сообщения, невозможно получить само сообщение
- C. Получение одинакового дайджеста из двух различных сообщений невозможно, либо случается крайне редко
- D. Она преобразует сообщение фиксированной длины в значение переменной длины

4. Что может указывать на изменение сообщения?

- A. Изменился открытый ключ
- B. Изменился закрытый ключ
- C. Изменился дайджест сообщения

D. Сообщение было правильно зашифровано

5. Какой из перечисленных ниже алгоритмов является алгоритмом американского правительства, предназначенным для создания безопасных дайджестов сообщений?

A. Data Encryption Algorithm

B. Digital Signature Standard

C. Secure Hash Algorithm

D. Data Signature Algorithm

6. Что из перечисленного ниже лучше всего описывает отличия между HMAC и CBC-MAC?

A. HMAC создает дайджест сообщения и применяется для контроля целостности; CBC-MAC используется для шифрования блоков данных с целью обеспечения конфиденциальности

B. HMAC использует симметричный ключ и алгоритм хэширования; CBC-MAC использует первый блок в качестве контрольной суммы

C. HMAC обеспечивает контроль целостности и аутентификацию источника данных; CBC-MAC использует блочный шифр в процессе создания MAC

D. HMAC зашифровывает сообщение на симметричном ключе, а затем передает результат в алгоритм хэширования; CBC-MAC зашифровывает все сообщение целиком

7. В чем преимущество RSA над DSA?

A. Он может обеспечить функциональность цифровой подписи и шифрования

B. Он использует меньше ресурсов и выполняет шифрование быстрее, поскольку использует симметричные ключи

C. Это блочный шифр и он лучше поточного

D. Он использует одноразовые шифровальные блокноты

8. Многие страны ограничивают использование и экспорт криптографических систем. Зачем они это делают?

A. Без ограничений может возникнуть большое число проблем совместимости при попытке использовать различные алгоритмы в различных программах

B. Эти системы могут использоваться некоторыми странами против их местного населения

C. Криминальные элементы могут использовать шифрование, чтобы избежать обнаружения и преследования

D. Законодательство сильно отстает, а создание новых типов шифрования еще больше усиливает эту проблему

9. Что используется для создания цифровой подписи?

- A. Закрытый ключ получателя
- B. Открытый ключ отправителя
- C. Закрытый ключ отправителя
- D. Открытый ключ получателя

10. Что из перечисленного ниже лучше всего описывает цифровую подпись?

- A. Это метод переноса собственноручной подписи на электронный документ
- B. Это метод шифрования конфиденциальной информации
- C. Это метод, обеспечивающий электронную подпись и шифрование
- D. Это метод, позволяющий получателю сообщения проверить его источник и убедиться в целостности сообщения

11. Какова эффективная длина ключа в DES?

- A. 56
- B. 64
- C. 32
- D. 16

12. По какой причине удостоверяющий центр отзывает сертификат?

- A. Если открытый ключ пользователя скомпрометирован
- B. Если пользователь переходит на использование модели РЕМ, которая использует сеть доверия
- C. Если закрытый ключ пользователя скомпрометирован
- D. Если пользователь переходит работать в другой офис

13. Что из перечисленного ниже лучше всего описывает удостоверяющий центр?

- A. Организация, которая выпускает закрытые ключи и соответствующие алгоритмы
- B. Организация, которая проверяет процессы шифрования

C. Организация, которая проверяет ключи шифрования

D. Организация, которая выпускает сертификаты

14. Как расшифровывается аббревиатура DEA?

A. Data Encoding Algorithm

B. Data Encoding Application

C. Data Encryption Algorithm

D. Digital Encryption Algorithm

15. Кто участвовал в разработке первого алгоритма с открытыми ключами?

A. Ади Шамир

B. Росс Андерсон

C. Брюс Шнайер

D. Мартин Хеллман

16. Какой процесс обычно выполняется после создания сеансового ключа DES?

A. Подписание ключа

B. Передача ключа на хранение третьей стороне (key escrow)

C. Кластеризация ключа

D. Обмен ключом

17. Сколько циклов перестановки и замещения выполняет DES?

A. 16

B. 32

C. 64

D. 56

18. Что из перечисленного ниже является правильным утверждением в отношении шифрования данных, выполняемого с целью их защиты?

A. Оно обеспечивает проверку целостности и правильности данных

- B. Оно требует внимательного отношения к процессу управления ключами
- C. Оно не требует большого количества системных ресурсов
- D. Оно требует передачи ключа на хранение третьей стороне (escrowed)

19. Как называется ситуация, в которой при использовании различных ключей для шифрования одного и того же сообщения в результате получается один и тот же шифротекст?

- A. Коллизия
- B. Хэширование
- C. MAC
- D. Кластеризация ключей

20. Что из перечисленного ниже является определением фактора трудозатрат для алгоритма?

- A. Время зашифрования и расшифрования открытого текста
- B. Время, которое займет взлом шифрования
- C. Время, которое занимает выполнение 16 циклов преобразований
- D. Время, которое занимает выполнение функций подстановки

21. Что является основной целью использования одностороннего хэширования пароля пользователя?

- A. Это снижает требуемый объем дискового пространства для хранения пароля пользователя
- B. Это предотвращает ознакомление кого-либо с открытым текстом пароля
- C. Это позволяет избежать избыточной обработки, требуемой асимметричным алгоритмом
- D. Это предотвращает атаки повтора (replay attack)

22. Какой из перечисленных ниже алгоритмов основан на сложности разложения больших чисел на два исходных простых множителя?

- A. ECC
- B. RSA
- C. DES
- D. Диффи-Хеллман

23. Что из перечисленного ниже описывает разницу между алгоритмами DES и RSA?

- A. DES – это симметричный алгоритм, а RSA – асимметричный
- B. DES – это асимметричный алгоритм, а RSA – симметричный
- C. Они оба являются алгоритмами хэширования, но RSA генерирует 160-битные значения хэша
- D. DES генерирует открытый и закрытый ключи, а RSA выполняет шифрование сообщений

24. Какой из перечисленных ниже алгоритмов использует симметричный ключ и алгоритм хэширования?

- A. HMAC
- B. 3DES
- C. ISAKMP-OAKLEY
- D. RSA

25. Генерация ключей, для которой используются случайные значения, называется Функцией генерации ключей (KDF). Какие значения обычно не используются при этом в процессе генерации ключей?

- A. Хэши
- B. Асимметричные значения
- C. Соль
- D. Пароли

Тема 4. Информационная безопасность пользователя

1) К правовым методам, обеспечивающим информационную безопасность, относятся:

- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
- + Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:

- Хищение жестких дисков, подключение к сети, инсайдерство
- + Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:

- + Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:

- + несанкционированного доступа, воздействия в сети

- инсайдерства в организации
- чрезвычайных ситуаций

5) Основные объекты информационной безопасности:

- + Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:

- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
- + Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:

- + Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:

- руководители, менеджеры, администраторы компаний
- + органы права, государства, бизнеса
- сетевые базы данных, фаерволлы

Тема 5. Терминологические основы информационной безопасности

Вопрос:

Основные угрозы конфиденциальности информации:

Варианты ответа:

- 1 (+) злоупотребления полномочиями

Вопрос:

Элементы знака охраны авторского права:

Варианты ответа:

- 1 (+) года первого выпуска программы

Вопрос:

Защита информации обеспечивается применением антивирусных средств

Варианты ответа:

- 1 - не всегда

Вопрос:

Средства защиты объектов файловой системы основаны на...

Варианты ответа:

- 1 - задании атрибутов файлов и каталогов, независящих от прав пользователей

Вопрос:

Вид угрозы действия, направленного на несанкционированное использование информационных ресурсов, не оказывающего при этом влияния на её функционирование — ... угроза

Варианты ответа:

- 1 (+) пассивная

Вопрос:

Преднамеренная угроза безопасности информации

Варианты ответа:

- 1 - ошибка разработчика

Вопрос:

Концепция системы защиты от информационного оружия не должна включать...

Варианты ответа:

- 1 - процедуры оценки уровня и особенностей атаки против национальной инфраструктуры в целом и отдельных пользователей

Вопрос:

В соответствии с нормами российского законодательства защита информации представляет собой принятие правовых, организационных и технических мер, направленных на ...

Варианты ответа:

- 1 - разработку методов и усовершенствование средств информационной безопасности

Вопрос:

Основные угрозы доступности информации:

Варианты ответа:

- 1 - перехват данных

Вопрос:

Суть компрометации информации

Варианты ответа:

- 1 (+) внесение несанкционированных изменений в базу данных, в результате чего потребитель вынужден либо отказаться от неё, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений

Вопрос:

Информационная безопасность автоматизированной системы – это состояние автоматизированной системы, при котором она, ...

Варианты ответа:

- 1 - способна противостоять только внешним информационным угрозам

Вопрос:

Методы повышения достоверности входных данных

Варианты ответа:

- 1 - Многократный ввод данных и сличение введенных значений

Вопрос:

Принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак (СОВ)

Варианты ответа:

- 1 - МЭ работают только на сетевом уровне, а СОВ – еще и на физическом

Вопрос:

Сервисы безопасности:

Варианты ответа:

- 1 - кэширование записей

Вопрос:

Под угрозой удаленного администрирования в компьютерной сети понимается угроза ...

Варианты ответа:

- 1 - поставки неприемлемого содержания

Вопрос:

Причины возникновения ошибки в данных

Варианты ответа:

- 1 (+) Ошибки при идентификации объекта или субъекта хозяйственной деятельности

Вопрос:

К формам защиты информации не относится...

Варианты ответа:

- 1 (+) страховая

Вопрос:

Наиболее эффективное средство для защиты от сетевых атак

Варианты ответа:

- 1 - использование только сертифицированных программ-броузеров при доступе к сети Интернет

Вопрос:

Информация, составляющая государственную тайну не может иметь гриф...

Варианты ответа:

- 1 - «особой важности»

Вопрос:

Разделы современной криптографии:

Варианты ответа:

- 1 (+) Управление ключами

Вопрос:

Документ, определивший важнейшие сервисы безопасности и предложивший метод классификации информационных систем по требованиям безопасности

Варианты ответа:

- 1 - Закону «Об информации, информационных технологиях и о защите информации»

Вопрос:

Утечка информации – это ...

Варианты ответа:

- 1 - непреднамеренная утрата носителя информации

Тема 6. Нормативно-правовое обеспечение информационной безопасности в РФ.

Вопрос 1

Как называется в гражданском кодексе РФ совокупность данных и команд, представленная в объективной форме и предназначенная для функционирования ЭВМ и других компьютерных устройств с целью получения определённого результата?

Выберите один из 4 вариантов ответа:

Варианты ответов

- Программа
- Утилита
- Алгоритм
- Приложение

Вопрос 2

Как называется информация в электронной форме, которая присоединена к другой информации в электронной форме, используемая для определения лица, подписавшего информацию?

Выберите один из 4 вариантов ответа:

Варианты ответов

- Договор
- Электронная подпись
- Антивирусная программа
- Блог

Вопрос 3

Какие из средств защиты информации направлены на защиту оборудования?

Выберите один из 4 вариантов ответа:

Варианты ответов

- Программные
- Аппаратные

- Физические
- Организационные

Вопрос 4

Установите соответствие между программными средствами информационной безопасности и их описанием.

Укажите соответствие для всех 3 вариантов ответа:

Варианты ответов

- Фильтрует трафик между компьютером и сетью
- Обеспечивает сохранность информации
- Ищет и удаляет вредоносный код

Вопрос 5

Установите соответствие между составляющими информационной безопасности и их определениями.

Укажите соответствие для всех 3 вариантов ответа:

Варианты ответов

- Неизменность информации, при выполнении некоторых операций над ней
- Требование не передавать информацию третьим лицам
- Возможность субъектов воспользоваться своими правами доступа к информации

Вопрос 6

Как называется состояние информационной среды, в котором обеспечены конфиденциальность, целостность и доступность информации?

Выберите один из 4 вариантов ответа:

Варианты ответов

- Информационная свобода
- Информационное общество
- Информационная защищённость
- Информационная безопасность

Вопрос 7

Сколько статей в разделе "Преступления в сфере компьютерной информации" уголовного кодекса РФ?

Запишите число:

Варианты ответов

- 1
- 2
- 3

Тема 7. Структура информационной безопасности, применяемая в общемировой практике

Тестовые задания

- 1 Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это....
- 2 **информационная война**
- 3 информационное оружие
- 4 информационное превосходство

- 5 Информация не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения в преимущественное положение по сравнению с другими объектами.
- 6 служебная информация
- 7 коммерческая тайна
- 8 банковская тайна
- 9 **конфиденциальная информация**
- 10 Гарантия того, что конкретная информация доступна только тому кругу лиц, для которых она предназначена
- 11 **конфиденциальность**
- 12 целостность
- 13 доступность
- 14 аутентичность
- 15 апеллируемость
- 16 Гарантия того, что АС ведет себя в нормальном и внештатном режиме так, как запланировано
- 17 **надежность**
- 18 точность
- 19 контролируемость
- 20 устойчивость
- 21 доступность
- 22 Способность системы к целенаправленному приспособлению при изменении структуры, технологических схем или условий функционирования, которое спасает владельца АС от необходимости принятия кардинальных мер по полной замене средств защиты на новые.
- 23 принцип системности
- 24 принцип комплексности
- 25 принцип непрерывной защиты
- 26 принцип разумной достаточности
- 27 **принцип гибкости системы**
- 28 В классификацию вирусов по способу заражения входят
- 29 опасные
- 30 файловые
- 31 **резидентные**
- 32 загрузочные
- 33 файлово -загрузочные
- 34 **нерезидентные**
- 35 Комплекс превентивных мер по защите конфиденциальных данных и информационных процессов на предприятии это...
- 36 **комплексное обеспечение ИБ**
- 37 безопасность АС
- 38 угроза ИБ
- 39 атака на АС
- 40 политика безопасности
- 41 Вирусы, не связывающие свои копии с файлами, а создающие свои копии на дисках, не изменяя других файлов, называются:
- 42 компаньон - вирусами
- 43 **черви**
- 44 паразитические
- 45 студенческие
- 46 призраки
- 47 стелс - вирусы

- 48 макровирусы
- 49 К видам системы обнаружения атак относятся :
- 50 системы, обнаружения атаки на ОС
- 51 системы, обнаружения атаки на конкретные приложения
- 52 системы, обнаружения атаки на удаленных БД
- 53 **все варианты верны**
- 54 Автоматизированная система должна обеспечивать
- 55 надежность
- 56 **доступность**
- 57 **целостность**
- 58 контролируемость

Тема 8. Угрозы информационной безопасности

Основная масса угроз информационной безопасности приходится на:

- [+] а) Троянские программы
- [-] б) Шпионские программы
- [-] в) Черви

Какой вид идентификации и аутентификации получил наибольшее распространение:

- [-] а) системы PKI
- [+] б) постоянные пароли
- [-] в) одноразовые пароли

Под какие системы распространение вирусов происходит наиболее динамично:

- [-] а) Windows
- [-] б) Mac OS
- [+] в) Android

Заключительным этапом построения системы защиты является:

- [+] а) сопровождение
- [-] б) планирование
- [-] в) анализ уязвимых мест

Какие угрозы безопасности информации являются преднамеренными:

- [-] а) ошибки персонала
- [-] б) открытие электронного письма, содержащего вирус
- [+] в) не авторизованный доступ

Какой подход к обеспечению безопасности имеет место:

- [-] а) теоретический
- [+] б) комплексный
- [-] в) логический

Системой криптографической защиты информации является:

- [-] а) BFox Pro
- [-] б) CAudit Pro
- [+] в) Крипто

Про Какие вирусы активизируются в самом начале работы с операционной системой:

- [+] а) загрузочные вирусы
- [-] б) троянцы
- [-] в) черви

Stuxnet – это:

- [-] а) троянская программа
- [-] б) макровирус
- [+] в) промышленный вирус

Таргетированная атака – это:

[-] а) атака на сетевое оборудование

[+] б) атака на компьютерную систему крупного предприятия

[-] в) атака на конкретный компьютер пользователя

4.3 Промежуточная аттестация по дисциплине проводится в форме экзамена

Типовые вопросы экзамена (ОПК-9)

- 1 Теория защиты информации. Основные направления
- 2 Виды угроз. Основные нарушения.
- 3 Общая модель воздействия на информацию.
- 4 Общая модель процесса нарушения физической целостности информации.
- 5 Методы определения требований к защите информации.
- 6 Допущения в моделях оценки уязвимости информации.
- 7 Классификация требований к средствам защиты информации.
- 8 Способы и средства защиты информации.
- 9 Способы «абсолютной системы защиты».

Типовые задания для экзамена (ОПК-9)

- 1 Содержание интересов личности, общества и государства в информационной сфере.
- 2 Источники и содержание угроз в информационной сфере.
- 3 Классы информационных ресурсов.

4.4. Шкала оценивания промежуточной аттестации

| Оценка | Компетенции | Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата) |
|-----------------------------------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| «отлично» (85 - 100 баллов) | ОПК-9 | Показывает высокий уровень знаний в области технологий защиты информации в правоохранительной сфере. ¶Анализирует существующие методики определений требования к защите информации. ¶Демонстрирует знание принципов технологий защиты информации в правоохранительной сфере. ¶Способен осуществлять подробный подбор научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности. ¶ Свободно ориентируется в законодательстве РФ по защите информации. ¶ |
| «хорошо» (70 - 84 баллов) | ОПК-9 | Показывает хороший уровень знаний в области технологий защиты информации в правоохранительной сфере. ¶Анализирует существующие методики определений требования к защите информации. ¶Демонстрирует знание принципов технологий защиты информации в правоохранительной сфере. ¶Способен осуществлять подбор научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности. ¶ |
| «удовлетворительно» (50 - 69 баллов) | ОПК-9 | Показывает низкий уровень знаний в области технологий защиты информации в правоохранительной сфере. ¶ Не анализирует существующие методики определений требования к защите информации. ¶Слабо ориентируется в законодательстве РФ по защите информации. ¶Не способен продемонстрировать современные подходы к технологиям и методам обеспечения ИБ. ¶ |

| | | |
|--------------------------------------------|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| «неудовлетворительно» (менее 50 баллов) | ОПК-9 | Не имеет знаний в области технологий защиты информации в право-охранительной сфере.¶ Не анализирует существующие методики определений требования к защите информации.¶ Не способен использо-вать программные сред-ства¶ |
|--------------------------------------------|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

5. Методические указания для обучающихся по освоению дисциплины (модуля)

5.1 Методические указания по организации самостоятельной работы обучающихся:

Приступая к изучению дисциплины, в первую очередь обучающимся необходимо ознакомиться содержанием рабочей программы дисциплины (РПД), которая определяет содержание, объем, а также порядок изучения и преподавания учебной дисциплины, ее раздела, части.

Для самостоятельной работы важное значение имеют разделы «Объем и содержание дисциплины», «Учебно-методическое и информационное обеспечение дисциплины» и «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы».

В разделе «Объем и содержание дисциплины» указываются все разделы и темы изучаемой дисциплины, а также виды занятий и планируемый объем в академических часах.

В разделе «Учебно-методическое и информационное обеспечение дисциплины» указана рекомендуемая основная и дополнительная литература.

В разделе «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы» содержится перечень профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины.

5.2 Рекомендации обучающимся по работе с теоретическими материалами по дисциплине

При изучении и проработке теоретического материала необходимо:

- просмотреть еще раз презентацию лекции в системе MOODLe, повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной дополнительной литературы;
- при самостоятельном изучении теоретической темы сделать конспект, используя рекомендованные в РПД источники, профессиональные базы данных и информационные справочные системы;
- ответить на вопросы для самостоятельной работы, по теме представленные в пункте 3.2 РПД.
- при подготовке к текущему контролю использовать материалы фонда оценочных средств (ФОС).

5.3 Рекомендации по работе с научной и учебной литературой

Работа с основной и дополнительной литературой является главной формой самостоятельной работы и необходима при подготовке к устному опросу на семинарских занятиях, к дебатам, тестированию, экзамену. Она включает проработку лекционного материала и рекомендованных источников и литературы по тематике лекций.

Конспект лекции должен содержать реферативную запись основных вопросов лекции, в том числе с опорой на размещенные в системе MOODLe презентации, основных источников и литературы по темам, выводы по каждому вопросу. Конспект может быть выполнен в рамках распечатки выдачи презентаций лекций или в отдельной тетради по предмету. Он должен быть аккуратным, хорошо читаемым, не содержать не относящуюся к теме информацию или рисунки.

Конспекты научной литературы при самостоятельной подготовке к занятиям должны содержать ответы на каждый поставленный в теме вопрос, иметь ссылку на источник информации с обязательным указанием автора, названия и года издания используемой научной литературы. Конспект может быть опорным (содержать лишь основные ключевые позиции), но при этом позволяющим дать полный ответ по вопросу, может быть подробным. Объем конспекта определяется самим студентом.

В процессе работы с основной и дополнительной литературой студент может:

- делать записи по ходу чтения в виде простого или развернутого плана (создавать перечень основных вопросов, рассмотренных в источнике);
- составлять тезисы (цитирование наиболее важных мест статьи или монографии, короткое изложение основных мыслей автора);

- готовить аннотации (краткое обобщение основных вопросов работы);
- создавать конспекты (развернутые тезисы).

5.4. Рекомендации по подготовке к отдельным заданиям текущего контроля

Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.

Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:

- правильность ответа по содержанию;
- полнота и глубина ответа;
- сознательность ответа;
- логика изложения материала;
- рациональность использованных приемов и способов решения поставленной учебной задачи;
- своевременность и эффективность использования наглядных пособий и технических средств при ответе;
- использование дополнительного материала;
- рациональность использования времени, отведенного на задание.

Устный опрос может сопровождаться презентацией, которая подготавливается по одному из вопросов практического занятия. При выступлении с презентацией необходимо обращать внимание на такие моменты как:

- содержание презентации: актуальность темы, полнота ее раскрытия, смысловое содержание, соответствие заявленной темы содержанию, соответствие методическим требованиям (цели, ссылки на ресурсы, соответствие содержания и литературы), практическая направленность, соответствие содержания заявленной форме, адекватность использования технических средств учебным задачам, последовательность и логичность презентуемого материала;
- оформление презентации: объем (оптимальное количество), дизайн (читаемость, наличие и соответствие графики и анимации, звуковое оформление, структурирование информации, соответствие заявленным требованиям), оригинальность оформления, эстетика, использование возможности программной среды, соответствие стандартам оформления;
- личностные качества: ораторские способности, соблюдение регламента, эмоциональность, умение ответить на вопросы, систематизированные, глубокие и полные знания по всем разделам программы;
- содержание выступления: логичность изложения материала, раскрытие темы, доступность изложения, эффективность применения средств ИКТ, способы и условия достижения результативности и эффективности для выполнения задач своей профессиональной или учебной деятельности, доказательность принимаемых решений, умение аргументировать свои заключения, выводы.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература:

1. Передков В.М., Митрошкин А.Г. Информационная безопасность и защита информации. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)
2. Лопатин Д.В., Калинина Ю.В. Безопасные информационные технологии : электрон. учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)
3. Тамб гос. ун-т им. Г.Р. Державина, Ин-т математики, физики и информатики Техническая защита информации : учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)

6.2 Дополнительная литература:

1. Загинайлов Ю. Н. Основы информационной безопасности: курс визуальных лекций : учебное пособие. - Москва|Берлин: Директ-Медиа, 2015. - 105 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=362895>
2. Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие. - Москва|Берлин: Директ-Медиа, 2015. - 253 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=276557>
3. Аверченков В. И., Рытов М. Ю., Кувыклин А. В., Рудановский М. В. Аудит информационной безопасности органов исполнительной власти : учебное пособие. - 4-е изд., стер.. - Москва: Флинта, 2016. - 100 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=93259>
4. Аверченков, В. И., Рытов, М. Ю., Кувыклин, А. В., Рудановский, М. В. Аудит информационной безопасности органов исполнительной власти : учебное пособие. - Весь срок охраны авторского права; Аудит информационной безопасности органов исполнительной власти. - Брянск: Брянский государственный технический университет, 2012. - 100 с. - Текст : электронный // IPR BOOKS [сайт]. - URL: <http://www.iprbookshop.ru/6992.html>
5. Комплексное обеспечение информационной безопасности автоматизированных систем : лабораторный практикум. - Ставрополь: Северо-Кавказский Федеральный университет (СКФУ), 2016. - 242 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=458012>

6.3 Иные источники:

1. Курс «Стандарты информационной безопасности» - <https://www.intuit.ru/studies/courses/30/30/info>
2. Курс «Основы информационной безопасности» - <https://www.intuit.ru/studies/courses/10/10/info>

7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы

Для проведения занятий по дисциплине необходимо следующее материально-техническое обеспечение: учебные аудитории для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещения для самостоятельной работы.

Учебные аудитории и помещения для самостоятельной работы укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы укомплектованы компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета.

Для проведения занятий лекционного типа используются наборы демонстрационного оборудования, обеспечивающие тематические иллюстрации (проектор, ноутбук, экран/ интерактивная доска).

Лицензионное и свободно распространяемое программное обеспечение:

Kaspersky Endpoint Security для бизнеса - Стандартный Russian Edition. 1500-2499 Node 1 year Educational Renewal Licence

Операционная система Microsoft Windows 10

Adobe Reader XI (11.0.08) - Russian Adobe Systems Incorporated 10.11.2014 187,00 MB 11.0.08

7-Zip 9.20

Microsoft Office Профессиональный плюс 2007

Профессиональные базы данных и информационные справочные системы:

1. Электронный каталог Фундаментальной библиотеки ТГУ. – URL: <http://biblio.tsutmb.ru/elektronnyij-katalog>

2. Университетская библиотека онлайн: электронно-библиотечная система. – URL: <https://biblioclub.ru>
3. Консультант студента. Гуманитарные науки: электронно-библиотечная система. – URL: <https://www.studentlibrary.ru>
4. Научная электронная библиотека eLIBRARY.ru. – URL: <https://elibrary.ru>
5. Российская государственная библиотека. – URL: <https://www.rsl.ru>
6. Российская национальная библиотека. – URL: <http://nlr.ru>
7. Научная электронная библиотека Российской академии естествознания. – URL: <https://www.monographies.ru>
8. Президентская библиотека имени Б.Н. Ельцина. – URL: <https://www.prlib.ru>
9. Электронная библиотека РФФИ. – URL: <https://www.rfbr.ru/rffi/ru/library>

Электронная информационно-образовательная среда

https://auth.tsutmb.ru/authorize?response_type=code&client_id=moodle&state=xyz

Взаимодействие преподавателя и студента в процессе обучения осуществляется посредством мультимедийных, гипертекстовых, сетевых, телекоммуникационных технологий, используемых в электронной информационно-образовательной среде университета.