МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

**Федеральное государственное бюджетное образовательное**

**учреждение высшего образования**

**К Г Э У «КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭНЕРГЕТИЧЕСКИЙ**

**УНИВЕРСИТЕТ»**

(ФГБОУ ВО «КГЭУ»)

УТВЕРЖДАЮ

Директор ИЦТЭ

\_\_\_\_\_\_\_\_\_\_ Ю.Н. Смирнов

«\_\_29\_\_» \_\_\_\_05\_\_\_2017 г.

# 

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации студентов по итогам освоения дисциплины

**Б1.О.22 Информационная безопасность**

(код, наименование дисциплины)

основной образовательной программы

Прикладная информатика в экономике

(наименование ООП)

по направлению подготовки

09.03.03 Прикладная информатика

(шифр, наименование направления подготовки)

Квалификация выпускника

бакалавр

(бакалавр, магистр)

Форма(ы) обучения

очная

(очная, очно-заочная, заочная)

Казань – 2017 г.

## 1. Цель и задачи текущего контроля и промежуточной аттестации студентов по дисциплине «Информационная безопасность»

Целью текущего контроля и промежуточной аттестации является развитие у студентов навыков работы с учебной и научной литературой, проведения учебно-исследовательской работы, а также для систематизации знаний по курсу при изучении методов и средств защиты информации, обеспечения ее конфиденциальности, целостности и доступности в процессе хранения и передачи: криптографических алгоритмов и протоколов, протоколов и систем аутентификации, электронной цифровой подписи, технологий межсетевых экранов и виртуальных частных сетей.

Задачами текущего контроля и текущей аттестации является углубление и закрепление знаний у студентов и развитие у них практических умений.

*Цель текущего контроля* – систематическая проверка степени освоения программы дисциплины «Защита информации», уровня сформированности знаний, умений, навыков, компетенций на текущих занятиях

*Задачи текущего контроля:*

1. определение индивидуального учебного рейтинга студентов;
2. своевременное выполнение корректирующих действий по содержанию и организации процесса обучения; обнаружение и устранение пробелов в усвоении учебной дисциплины;
3. подготовки к промежуточной аттестации.

В течение семестра при изучении дисциплины реализуется комплексная система поэтапного оценивания уровня освоения – балльно-рейтинговая система. За каждый вид учебных действий студенты получают определенное количество баллов. В течение семестра студент может набрать от 35 до 60-ти баллов в зависимости от уровня освоения программы образования: базового, продвинутого и высокого.

*Цель промежуточной аттестации* – проверка степени усвоения студентами учебного материала за время изучения дисциплины, уровня сформированности компетенций после завершения изучения дисциплины. Аттестация проходит в форме экзамена. Учитывая специфические особенности дисциплины и степень её важности, экзамен проводится в устной форме с элементами собеседования. Экзаменационные билеты содержат три теоретических вопроса.

При полном ответе на все задания студент получает до 40 баллов.

*Задачи промежуточной аттестации:*

1. определение уровня усвоения учебной дисциплины;
2. определение уровня сформированности элементов общекультурных и профессиональных компетенций.

## 2. Основное содержание текущего контроля и промежуточной аттестации студентов

В результате изучения дисциплины «Информационная безопасность» формируются следующие компетенции или их составляющие:

* способен находить организационно-управленческие решения и готов нести за них от-ветственность (ОК-4);
* способен работать с информацией в глобальных компьютерных сетях (ОК-8);
* способен понимать сущность и значение информации в развитии современного ин-формационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны (ОК-13);
* способен использовать нормативные правовые документы в профессиональной дея-тельности (ПК-1);
* способен осуществлять и обосновывать выбор проектных решений по видам обеспече-ния информационных систем (ПК-5);
* способен принимать участие во внедрении, адаптации и настройке прикладных ИС

(ПК-13);

* способен оценивать и выбирать современные операционные среды и информационно-коммуникационные технологии для информатизации и автоматизации решения прикладных задач и создания ИС (ПК-16);
* способен применять методы анализа прикладной области на концептуальном, логиче-ском, математическом и алгоритмическом уровнях (ПК-17);
* способен анализировать и выбирать методы и средства обеспечения информационной безопасности (ПК-18);
* способен применять системный подход и математические методы в формализации ре-шения прикладных задач (ПК-21);
* способен готовить обзоры научной литературы и электронных информационнообразовательных ресурсов для профессиональной деятельности (ПК-22).

### 2.1. Основное содержание текущего контроля

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Коды ком-  петен-  ций | Совокупность ожидаемых результатов образования студентов в форме компетенций по завершении модуля / освоения  дисциплины | Содержание оценочных заданий для выявления сформированности компетенций у студентов по завершении модуля/освоения  дисциплины | | |
| Базовый уровень | Продвинутый уровень | Высокий уровень |
| 1 | 2 | 3 | 4 | 5 |
| **Общекультурные компетенции** | | | | |
| ОК-4 | ***Знать*:**   * цели, задачи, принципы и основные направления обеспе-чения информационной безопасности личности, общества, государства.   ***Уметь*:**   * выявлять и классифицировать угрозы информационной безопасности.   ***Владеть*:**   * навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем. | Тест | Тест | Контрольная работа |
| ОК-8 | ***Знать*:**   * компьютерную систему, как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности.   ***Уметь*:**   * разрабатывать политики информационной безопасности организации; * реализовывать защиту информационных систем от ком-пьютерных вирусов и других вредоносных программ.   ***Владеть*:**   * правилами и приемами защиты сведений, составляющих государственную тайну, коммерческую тайну, а также персональных данных. | Тест | Тест | Контрольная работа |
| ОК-13 | ***Знать*:**   * основные термины по проблематике информационной безопасности; * правовые аспекты обеспечения информационной без-опасности; * угрозы информационной безопасности.   ***Уметь*:**   * выявлять и классифицировать угрозы информационной безопасности; * разрабатывать модели злоумышленников; * разрабатывать политики информационной безопасности организации. | Тест | Тест | Контрольная работа |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | 2 |  | 3 | 4 | 5 |
|  | ***Владеть*:**  – правилами и приемами защиты сведений, составляющих государственную тайну, коммерческую тайну, а также персональных данных. |  |  |  |  |
| **Профессиональные компетенции** | | |  | | |
| ПК-1 | ***Знать*:**   * основные термины по проблематике информационной безопасности; * правовые аспекты обеспечения информационной без-опасности.   ***Уметь*:**   * разрабатывать политики информационной безопасности организации.   ***Владеть*:**   * правилами и приемами защиты сведений, составляющих государственную тайну, коммерческую тайну, а также персональных данных. |  | Тест | Тест | Контрольная работа |
| ПК-5 | ***Знать*:**   * методологию создания систем защиты информации; * перспективные направления развития систем и методов защиты информации; * современные подходы к построению систем защиты ин-формации.   ***Уметь*:**   * применять методы и средства защиты конфиденциальной информации, включая криптографические средства.   ***Владеть*:**   * навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем. |  | Тест | Тест | Контрольная работа |
| ПК-13 | ***Знать*:**   * современные подходы к построению систем защиты ин-формации; * компьютерную систему, как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности.   ***Уметь*:**   * реализовывать защиту информационных систем от ком-пьютерных вирусов и других вредоносных программ; – применять методы и средства защиты конфиденциальной информации, включая криптографические средства.   ***Владеть*:**   * навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем. |  | Тест | Тест | Контрольная работа |
| ПК-16 | ***Знать*:**   * компьютерную систему, как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности.   ***Уметь*:**   * применять методы и средства защиты конфиденциальной информации, включая криптографические средства.   ***Владеть*:**   * навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем. |  | Тест | Тест | Контрольная работа |
| ПК-17 | ***Знать*:**   * методологию создания систем защиты информации; * перспективные направления развития систем и методов защиты информации; * современные подходы к построению систем защиты ин- |  | Тест | Тест | Контрольная работа |
| 1 | 2 | 3 | | 4 | 5 |
|  | формации.  ***Уметь*:**   * реализовывать защиту информационных систем от ком-пьютерных вирусов и других вредоносных программ.   ***Владеть*:**   * навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем; * правилами и приемами защиты сведений, составляющих государственную тайну, коммерческую тайну, а также персональных данных. |  | |  |  |
| ПК-18 | ***Знать*:**   * современные подходы к построению систем защиты ин-формации; * компьютерную систему, как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности.   ***Уметь*:**   * применять методы и средства защиты конфиденциальной информации, включая криптографические средства.   ***Владеть*:**   * навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем. | Тест | | Тест | Контрольная работа |
| ПК-21 | ***Знать*:**   * методологию создания систем защиты информации; * современные подходы к построению систем защиты ин-формации.   ***Уметь*:**   * разрабатывать политики информационной безопасности организации; * реализовывать защиту информационных систем от ком-пьютерных вирусов и других вредоносных программ.   ***Владеть*:**   * навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем; * правилами и приемами защиты сведений, составляющих государственную тайну, коммерческую тайну, а также персональных данных. | Тест | | Тест | Контрольная работа |
| ПК-22 | ***Знать*:**   * основные термины по проблематике информационной безопасности; * методологию создания систем защиты информации; * угрозы информационной безопасности; * современные подходы к построению систем защиты ин-формации.   ***Уметь*:**   * разрабатывать политики информационной безопасности организации; * реализовывать защиту информационных систем от ком-пьютерных вирусов и других вредоносных программ.   ***Владеть*:**   * навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем. | Тест | | Тест | Контрольная работа |

**2.2. Основное содержание промежуточной аттестации студентов**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Коды ком-  петенций | Совокупность ожидаемых результатов образования студентов в форме компетенций по завершении модуля / освоения  дисциплины | Содержание оценочных заданий для выявления сформированности компетенций у студентов по завершении модуля/освоения  дисциплины | | |
| Базовый уровень | Продвинутый уровень | Высокий  уровень |
| 1 | 2 | 3 | 4 | 5 |
| **Общекультурные компетенции** | | | | |
| ОК-4 | ***Знать*:**   * цели, задачи, принципы и основные направления обеспе-чения информационной безопасности личности, общества, государства.   ***Уметь*:**   * выявлять и классифицировать угрозы информационной безопасности.   ***Владеть*:**   * навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем. | Экзамен | Экзамен | Экзамен |
| ОК-8 | ***Знать*:**   * компьютерную систему, как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности.   ***Уметь*:**   * разрабатывать политики информационной безопасности организации; * реализовывать защиту информационных систем от ком-пьютерных вирусов и других вредоносных программ.   ***Владеть*:**   * правилами и приемами защиты сведений, составляющих государственную тайну, коммерческую тайну, а также персональных данных. | Экзамен | Экзамен | Экзамен |
| ОК-13 | ***Знать*:**   * основные термины по проблематике информационной безопасности; * правовые аспекты обеспечения информационной без-опасности; * угрозы информационной безопасности. ***Уметь*:** * выявлять и классифицировать угрозы информационной безопасности; * разрабатывать модели злоумышленников; * разрабатывать политики информационной безопасности организации.   ***Владеть*:**   * правилами и приемами защиты сведений, составляющих государственную тайну, коммерческую тайну, а также персональных данных. | Экзамен | Экзамен | Экзамен |
| **Профессиональные компетенции** | | | | |
| ПК-1 | ***Знать*:**   * основные термины по проблематике информационной безопасности; * правовые аспекты обеспечения информационной без-опасности. ***Уметь*:** * разрабатывать политики информационной безопасности организации.   ***Владеть*:**   * правилами и приемами защиты сведений, составляющих государственную тайну, коммерческую тайну, а также персональных данных. | Экзамен | Экзамен | Экзамен |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ПК-5 | ***Знать*:**   * методологию создания систем защиты информации; * перспективные направления развития систем и методов защиты информации; * современные подходы к построению систем защиты ин-формации.   ***Уметь*:**   * применять методы и средства защиты конфиденциальной информации, включая криптографические средства.   ***Владеть*:**   * навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем. | Экзамен | Экзамен | Экзамен |
| ПК-13 | ***Знать*:**   * современные подходы к построению систем защиты ин-формации; * компьютерную систему, как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности.   ***Уметь*:**   * реализовывать защиту информационных систем от ком-пьютерных вирусов и других вредоносных программ; – применять методы и средства защиты конфиденциальной информации, включая криптографические средства.   ***Владеть*:**   * навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем. | Экзамен | Экзамен | Экзамен |
| ПК-16 | ***Знать*:**   * компьютерную систему, как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности.   ***Уметь*:**   * применять методы и средства защиты конфиденциальной информации, включая криптографические средства.   ***Владеть*:**   * навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем. | Экзамен | Экзамен | Экзамен |
| ПК-17 | ***Знать*:**   * методологию создания систем защиты информации; * перспективные направления развития систем и методов защиты информации; * современные подходы к построению систем защиты ин-формации.   ***Уметь*:**   * реализовывать защиту информационных систем от ком-пьютерных вирусов и других вредоносных программ.   ***Владеть*:**   * навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем; * правилами и приемами защиты сведений, составляющих государственную тайну, коммерческую тайну, а также персональных данных. | Экзамен | Экзамен | Экзамен |
| ПК-18 | ***Знать*:**   * современные подходы к построению систем защиты ин-формации; * компьютерную систему, как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности.   ***Уметь*:**   * применять методы и средства защиты конфиденциальной | Экзамен | Экзамен | Экзамен |
|  | информации, включая криптографические средства.  ***Владеть*:**  – навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем. |  |  |  |
| ПК-21 | ***Знать*:**   * методологию создания систем защиты информации; * современные подходы к построению систем защиты ин-формации. ***Уметь*:** * разрабатывать политики информационной безопасности организации; * реализовывать защиту информационных систем от ком-пьютерных вирусов и других вредоносных программ.   ***Владеть*:**   * навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем; * правилами и приемами защиты сведений, составляющих государственную тайну, коммерческую тайну, а также персональных данных. | Экзамен | Экзамен | Экзамен |
| ПК-22 | ***Знать*:**   * основные термины по проблематике информационной безопасности; * методологию создания систем защиты информации; * угрозы информационной безопасности; * современные подходы к построению систем защиты ин-формации. ***Уметь*:** * разрабатывать политики информационной безопасности организации; * реализовывать защиту информационных систем от ком-пьютерных вирусов и других вредоносных программ.   ***Владеть*:**   * навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем. | Экзамен | Экзамен | Экзамен |

## 3. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации по итогам освоения дисциплины

Оценка текущей успеваемости и промежуточной аттестации студентов по итогам освоения дисциплины «Информационная безопасность» производится при помощи следующих оценочных средств:

### 3.1. Входной контроль

Входной контроль проводится в начале семестра. Он представляют собой тесты из 20 основных вопросов, ответы на которые студент должен знать в результате изучения предыдущих дисциплин. Контроль проводится по оценке остаточных знаний по дисциплинам «Программное обеспечение средств вычислительной техники», «Информатика и программирование». Поставленные вопросы требуют точных и коротких ответов. Входной контроль проводится в письменном виде на первой лекции семестра в течение 10-15 минут. Итоги входного контроля используются для корректировки методик проведения лекционных, лабораторных и практических занятий, а также для определения уровня освоения программы образования: базового, продвинутого и высокого. Однако студент в праве сам выбирать, по программе какого уровня будет выполняться его работа.

Критерием оценивания результатов является правильность ответа на задание.

Подсчитывается каждый правильный ответ студента. Для определения соответствия между количеством правильных ответов и приблизительным уровнем знаний студентов используется соответствующая таблица – для оценивания заданий входного уровня.

## Таблица - Шкала оценивания выполнения заданий

|  |  |  |
| --- | --- | --- |
| Количество правильных ответов | Оценка | Баллы |
| 9-10 | 5 | 15 |
| 6-8 | 4 | 12 |
| 3-5 | 3 | 9 |
| менее 3 | 2 | 0 |

Итоги входного контроля используются для корректировки методик проведения лекционных, лабораторных и практических занятий, а также для определения уровня освоения программы образования: базового, продвинутого и высокого. Однако студент в праве сам выбирать, по программе какого уровня будет выполняться его работа.

***Тестовые задания входного контроля:***

1. Укажите истинность или ложность вариантов ответа:

а) почтовый червь активируется в тот момент, когда к вам поступает электронная почта;

б) если компьютер не подключен к сети Интернет, в него не проникнут вирусы;

в) файловые вирусы заражают файлы с расширениями \*.doc, \*.ppt, \*.xls;

г) чтобы защитить компьютер недостаточно только установить антивирусную программу;

д) на Web-страницах могут находится сетевые черви.

1. К вредоносным программам относятся (выберите несколько вариантов ответа): а) потенциально опасные программы;

б) вирусы, черви, трояны;

в) шпионские и рекламные программы;

г) вирусы, программы-шутки, антивирусное программное обеспечение;

д) межсетевой экран, брандмауэр.

1. Сетевые черви это

а) вредоносные программы, устанавливающие скрытно от пользователя другие вредоносные программы и утилиты;

б) вирусы, которые проникнув на компьютер, блокируют работу сети;

в) вирусы, которые внедряются в документы под видом макросов;

г) хакерские утилиты, управляющие удаленным доступом компьютера;

д) вредоносные программы, которые проникают на компьютер, используя сервисы компьютерных сетей.

1. К биометрической системе защиты относятся (выберите несколько вариантов ответа): а) защита паролем;

б) физическая защита данных;

в) антивирусная защита;

г) идентификация по радужной оболочке глаз;

д) идентификация по отпечаткам пальцев.

1. Вредоносная программа, которая подменяет собой загрузку некоторых программ при загрузке системы, называется... а) загрузочный вирус;

б) макровирус;

в) троян;

г) сетевой червь;

д) файловый вирус.

1. Руткит – это...

а) вредоносная программа, выполняющая несанкционированные действия по передаче управления компьютером удаленному пользователю;

б) разновидность межсетевого экрана;

в) программа, использующая для распространения Рунет (Российскую часть Интернета);

г) вредоносная программа, маскирующаяся под макрокоманду;

д) программа для скрытого взятия под контроль взломанной системы.

1. Компьютерные вирусы это (выберите несколько из 5 вариантов ответа):

а) вредоносные программы, наносящие вред данным;

б) программы, уничтожающие данные на жестком диске;

в) программы, которые могут размножаться и скрыто внедрять свои копии в файлы, загрузочные сектора дисков, документы;

г) программы, заражающие загрузочный сектор дисков и препятствующие загрузке компьютера;

д) скрипты, помещенные на зараженных интернет-страницах.

1. Вирус внедряется в исполняемые файлы и при их запуске активируется – это... а) загрузочный вирус;

б) макровирус;

в) файловый вирус;

г) сетевой червь;

д) троян.

1. Укажите порядок действий при наличии признаков заражения компьютера (укажите порядок следования всех 3 вариантов ответа): а) сохранить результаты работы на внешнем носителе;

б) запустить антивирусную программу;

в) отключиться от глобальной или локальной сети.

1. Вирус, поражающий документы называется а) троян;

б) файловый вирус;

в) макровирус;

г) загрузочный вирус;

д) сетевой червь.

1. Незаконный сбор, присвоение и передача сведений составляющих коммерческую тайну, наносящий ее владельцу ущерб, – это... а) политическая разведка;

б) промышленный шпионаж;

в) добросовестная конкуренция;

г) конфиденциальная информация;

д) правильного ответа нет.

1. Что называют источником конфиденциальной информации?

а) объект, обладающий определенными охраняемыми сведениями, представляющими интерес для злоумышленни-

ков;

б) сведения о предметах, объектах, явлениях и процессах, отображаемые на каком-либо носителе;

в) доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники;

г) это защищаемые предприятием сведения в области производства и коммерческой деятельности;

д) способ, позволяющий нарушителю получить доступ к обрабатываемой или хранящейся в ПЭВМ информации.

1. Какие основные цели преследует злоумышленник при несанкционированном доступе к информации?

а) получить, изменить, а затем передать ее конкурентам;

б) размножить или уничтожить ее;

в) получить, изменить или уничтожить;

г) изменить и уничтожить ее;

д) изменить, повредить или ее уничтожить.

1. В каком варианте ответа инфекции расположены от более простого к более сложному, по возрастанию?

а) логические бомбы, троянский конь, червь, вирус;

б) червь, вирус логические бомбы, троянский конь;

в) червь логические бомбы вирус, троянский конь;

г) логические бомбы, вирус, троянский конь червь;

д) вирус, логические бомбы, троянский конь червь.

1. Какие средства использует инженерно-техническая защита (по функциональному назначению)?

а) программные, аппаратные, криптографические, технические;

б) программные, физические, шифровальные, криптографические;

в) программные, аппаратные, криптографические физические;

г) физические, аппаратные, материальные, криптографические;

д) аппаратные, физические, программные, материальные.

1. Что включают в себя технические мероприятия по защите информации?

а) поиск и уничтожение технических средств разведки;

б) кодирование информации или передаваемого сигнала;

в) подавление технических средств постановкой помехи;

г) применение детекторов лжи;

д) все вышеперечисленное.

1. Какие основные направления в защите персональных компьютеров от несанкционированного доступа Вы знаете?

а) недопущение нарушителя к вычислительной среде;

б) защита вычислительной среды;

в) использование специальных средств защиты информации ПК от несанкционированного доступа; г) все вышеперечисленные;

д) правильного ответа нет.

1. Какие средства защиты информации в ПК наиболее распространены?

а) применение различных методов шифрования, не зависящих от контекста информации;

б) средства защиты от копирования коммерческих программных продуктов;

в) средства защиты вычислительных ресурсов, использующие парольную идентификацию и ограничивающие доступ несанкционированного пользователя;

г) защита от компьютерных вирусов и создание архивов;

д) все вышеперечисленные.

1. Информацию, отражающую истинное положение дел, называют: а) понятной;

б) достоверной;

в) объективной;

г) полной;

д) полезной.

1. Информацию, существенную и важную в настоящий момент, называют: а) полезной;

б) актуальной;

в) достоверной;

г) объективной;

д) полной.

### 3.2. Контроль текущей самостоятельной работы

Данный вид контроля состоит из тестов, контрольных работ и допуска к экзамену по итогам выполнения лабораторных и практических работ. Тесты, контрольные работы, выполнение лабораторных и практических работ являются обязательной формой контроля.

Контроль текущей успеваемости проводится в конце каждого учебного модуля.

В начале последнего лабораторного или практического занятия учебного модуля на осуществление контроля отводится 10 минут. Студентам предлагается самостоятельно выполнить задания. Ответы записываются студентами на бумажном носителе.

В каждом учебном модуле студенту выдается задание состоящее из 3 позиций: 1 задание из базового уровня; 2 – из продвинутого; 3 – из высокого. За каждое правильно выполненное задание присваивается определенное количество процентов. Суммарно студент может получить до 100% согласно шкале оценивания результатов.

В каждом модуле дается 10 тестовых заданий, что соответствует базовому уровню, 5 задач для продвинутого уровня, и 5 задач и вопросов для высокого уровня.

Критерием оценивания результатов является правильность ответа на задание.

Каждый правильный ответ на тестовое задание оценивается в 0,5 балла. Каждый правильный ответ на вопросы и задачи продвинутого и высокого уровней оценивается в 1 балл.

Для определения соответствия между количеством набранных баллов и процентом выполнения заданий используется соответствующая таблица:

Критерии оценивания результатов

|  |  |  |
| --- | --- | --- |
| Номер задания | Критерии оценки | Проценты |
| 1 | Правильность выполнения тестовых заданий | 0-45 |
| 2 | Правильность выполнения контрольной работы | 0-25 |
| 3 | Правильность выполнения контрольной работы | 0-30 |

## Шкала оценивания результатов

|  |  |
| --- | --- |
| Оценка | Проценты |
| удовлетворительно | 35-50 |
| хорошо | 50-74 |
| отлично | 75-100 |

Набранные баллы потом учитываются при определении суммарного количества баллов за каждый учебный модуль.

### 3.2.1 Тесты и контрольные работы

Данный вид контроля представляет собой короткие задания, которые выполняются на лабораторных или практических занятиях в течение 10-15 минут. Проверяются знания текущего материала: знания основных алгоритмов шифрования, получения ЭЦП, общих вопросов защиты информации, особенностей корректирующих кодов, методов безопасной передачи информации по каналам связи. Текущий контроль проводится в конце каждого учебного модуля.

Для ***базового уровня*** он представляет собой тесты тест на знания основных алгоритмов шифрования, получения ЭЦП, общих вопросов защиты информации, особенностей корректирующих кодов, методов безопасной передачи информации по каналам связи. Тест может содержать один верный ответ.

## *Фонд тестовых заданий*

1. Открытый трафик – это:

а) поток пакетов, незашифрованных на сетевом и прикладном уровне;

б) поток пакетов, незашифрованных на сетевом уровне, причем данные могут быть зашифрованы на прикладном уровне;

в) поток пакетов, незашифрованных на прикладной уровне, причем данные могут быть зашифрованы на сетевом уровне;

г) поток пакетов от пакетов от компьютеров, не входящих в сеть ViPNet.

1. Меры, мероприятия и действия, которые должны осуществлять должностные лица в процессе работы с информацией для обеспечения заданного уровня ее безопасности, относятся к:

а) гражданско-правовым методам обеспечения информационной безопасности;

б) внутриобъектовым методам обеспечения информационной безопасности;

в) организационным методам обеспечения информационной безопасности;

г) правовым методам обеспечения информационной безопасности.

1. Путь несанкционированного распространения носителя информации от источника к злоумышленнику называется:

а) несанкционированным доступом к информации;

б) каналом утечки информации;

в) утечкой информации;

г) несанкционированным распространением информации.

1. Злонамеренный код обладает следующими отличительными чертами: не требует программы-носителя, вызывает распространение своих копий и их выполнение (для активизации вируса требуется запуск зараженной программы). Назовите тип этого злонамеренного кода. а) макровирус;

б) троянский конь;

в) червь;

г) файловый вирус.

1. На какие виды по физической природе подразделяются технические каналы утечки информации?

а) оптические;

б) видимые;

в) вещественные;

г) акустические;

д) разведывательные;

е) инфракрасные;

ж) радиоэлектронные.

1. К косвенным каналам утечки информации относятся:

а) кража или утеря носителей информации;

б) копирование защищаемой информации из информационной системы;

в) исследование не уничтоженного мусора;

г) перехват электромагнитных излучений;

д) инсайдерские действия.

1. Какие задачи информационной безопасности решаются на организационном уровне? а) внедрение системы безопасности;

б) разработка документации;

в) обучение персонала;

г) сертификация средств защиты информации;

д) ограничение доступа на объект;

е) внедрение системы контроля и управления доступом.

1. К источникам случайных воздействий можно отнести:

а) неисправные технические средства сбора, обработки, передачи и хранения информации б) ошибки персонала;

в) стихийные силы;

г) программы, содержащие вирусы;

д) действие создаваемых злоумышленником полей и сигналов.

1. По аспекту информационной безопасности угрозы классифицируются на:

а) угрозы нарушения конфиденциальности и секретности;

б) угрозы нарушения конфиденциальности, целостности, доступности;

в) угрозы нарушения конфиденциальности и криптографического скрытия;

г) угрозы нарушения криптографического скрытия.

1. Атака «man in the middle» является:

а) пассивной;

б) активной;

в) может быть как активной, так и пассивной;

г) нет верного ответа.

1. Межсетевой экран позволяет:

а) разделять сети друг от друга;

б) принимать решение о возможности дальнейшего направления трафика к пункту назначения;

в) проверять весь входящий и исходящий трафик;

г) все перечисленные выше варианты верны.

1. Что включают в себя технические мероприятия по защите информации?

а) поиск и уничтожение технических средств разведки;

б) кодирование информации или передаваемого сигнала;

в) подавление технических средств постановкой помехи;

г) применение детекторов лжи;

д) все вышеперечисленное.

1. Алгоритм RSA основан на:

а) задаче дискретного логарифмирования;

б) задаче факторизации числа;

в) задаче определения, является ли данное число простым;

г) нет верного ответа.

1. Алгоритм ГОСТ 28147:

а) имеет переменную длину ключа;

б) основан на сети Фейcтеля;

в) разбивает блок на фиксированные 16-битные подблоки;

г) нет верного ответа.

1. Алгоритм Диффи-Хеллмана дает возможность:

а) безопасно обменяться общим секретом;

б) безопасно обменяться общим секретом при условии аутентификации сторон;

в) подписать сообщение;

г) нет верного ответа.

1. Алгоритм Диффи-Хеллмана основан на:

а) задаче дискретного логарифмирования;

б) задаче факторизации числа;

в) задаче определения, является ли данное число простым;

г) нет верного ответа.

1. Алгоритм симметричного шифрования называется блочным, если:

а) алгоритм основан на сети Фейстеля;

б) для шифрования исходный текст разбивается на блоки фиксированной длины;

в) в алгоритме используются S-box;

г) нет верного ответа.

1. Аутентификация – это:

а) невозможность несанкционированного доступа к данным;

б) подтверждение того, что информация получена из законного источника законным получателем;

в) невозможность несанкционированного просмотра и модификации информации;

г) нет верного ответа.

1. В DSS используется следующая хэш-функция: а) MD5;

б) SHA-1;

в) SHA-2;

г) нет верного ответа.

1. В алгоритмах симметричного шифрования используются только следующие операции:

а) операции перестановки и сдвига;

б) S-box и побитовое исключающее или (XOR);

в) любые из перечисленных выше операций, а также многие другие;

г) нет верного ответа.

1. Информация, составляющая государственную тайну не может иметь гриф… а) «особой важности»

б) «совершенно секретно»

в) «для служебного пользования»

г) «секретно»

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

а) с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на её функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации б) способна противостоять только внешним информационным угрозам

в) с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды

г) способна противостоять только информационным угрозам, как внешним так и внутренним

1. Преднамеренная угроза безопасности информации а) наводнение

б) повреждение кабеля, по которому идет передача, в связи с погодными условиями в) ошибка разработчика

г) кража

1. Документ, определивший важнейшие сервисы безопасности и предложивший метод классификации информационных систем по требованиям безопасности а) рекомендации X.800

б) Закону «Об информации, информационных технологиях и о защите информации» в) Оранжевая книга

1. Основные угрозы доступности информации (можно выбрать 1 или несколько вариантов ответа):

а) отказ программного и аппаратно обеспечения

б) непреднамеренные ошибки пользователей

в) разрушение или повреждение помещений

г) злонамеренное изменение данных

д) перехват данных

е) хакерская атака

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

(можно выбрать 1 или несколько вариантов ответа)

а) выявление нарушителей и привлечение их к ответственности

б) соблюдение норм международного права в сфере информационной безопасности

в) разработку методов и усовершенствование средств информационной безопасности

г) реализацию права на доступ к информации»

д) соблюдение конфиденциальности информации ограниченного доступа

е) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации

1. Принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак

(СОВ)

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

б) МЭ были разработаны для активной или пассивной защиты, а СОВ – для активного или пассивного обнаружения

в) МЭ были разработаны для активного или пассивного обнаружения, а СОВ – для активной или пассивной защиты

1. К формам защиты информации не относится…

а) организационно-техническая

б) страховая

в) аналитическая

г) правовая

1. Утечка информации – это …

а) процесс раскрытия секретной информации

б) непреднамеренная утрата носителя информации

в) несанкционированный процесс переноса информации от источника к злоумышленнику процесс уничтожения информации

1. Средства защиты объектов файловой системы основаны на…

а) определении прав пользователя на операции с файлами и каталогами

б) задании атрибутов файлов и каталогов, независящих от прав пользователей

1. Защита информации обеспечивается применением антивирусных средств а) не всегда

б) нет

в) да

1. Под угрозой удаленного администрирования в компьютерной сети понимается угроза

…

а) перехвата или подмены данных на путях транспортировки

б) вмешательства в личную жизнь

в) поставки неприемлемого содержания

г) несанкционированного управления удаленным компьютером

д) внедрения агрессивного программного кода в рамках активных объектов Web-страниц

1. Суть компрометации информации

а) внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации

б) 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

в) несанкционированный доступ к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений

1. Сервисы безопасности:

а) экранирование

б) контроль целостности

в) обеспечение безопасного восстановления

г) кэширование записей

д) шифрование

е) регулирование конфликтов

ж) идентификация и аутентификация

з) инверсия паролей

1. Какие из перечисленных ниже алгоритмов не являются симметричными?

а) Подстановочные шифры (простой подстановочный шифр, или моноалфавитный шифр, однозвучный подстановочный шифр, полиграммный подстановочный шифр, полиалфавитный подстановочный шифр)

б) Перестановочные шифры (шифром перестановки, шифры с фигурами перестановки, использующие некоторую геометрическую фигуру, маршрутной перестановкой, поворотная решетка, шифр вертикальной перестановки) в).Шифры гаммирования.

г).Блочного шифры: DES (Data Encription Standart), TripleDES (3DES), AES (Advanced Encryption Standart), он же RIJNDAEL, SERPENT, TWOFISH, RC6, MARS, ГОСТ 28147-89, Blowfish. (P.S больше вспомнить не могу, если что-то еще кто-то припомнит, то напишите..) д) Поточные шифры.

1. Какую длину имеет секретный ключ в криптосистеме DES?

1. Блочные криптоалгоритмы в ходе своей производят преобразование…

1. Что такое раунд (round)?

1. Какая процедура распределения ключей не требует использования защищенного канала для передачи секретного ключа адресату?

1. Какая из систем с открытым ключом используется исключительно для генерации цифровой подписи?

1. Какие трудноразрешимые задачи используются для повышения стойкости алгоритма RSA?

1. Чему равен результат вычисления хэш-функции по алгоритму SHA-1?

1. Что такое двухфакторная аутентификация

1. Петр, находясь в сети организации, перевел свою сетевую карту в режим монитора для прослушивания пакетов. Какой вид атаки осуществляет Петр? а) Отказ в обслуживании

б) Фишинг

в) Снифинг

г) Активный спуфинг

д) Пассивный спуфинг

1. Какой сервис не реализовывает VPN-тунель?

а) Обеспечение отказоустойчивости канала связи

б) Обеспечение конфиденциальности информации

в) Обеспечение целостности информации

г) Обеспечение аутентификации пользователей

д) Предотвращение отказа от авторства

1. Что из перечисленного не используется в биометрической аутентификации? а) Рисунок папиллярного узора

б) Радужная оболочка глаза

в) PIN-код

г) Клавиатурный почерк

д) Пластиковая карта с магнитной полосой

1. Что лежит в основе мандатных политик безопасности? а) Таблицы доступа

б) Роли

в) Метки секретности

г) Нет верного ответа

д) Матрицы доступа

1. Какой из перечисленных паролей является наиболее надежным для пользователя admin?

а) pa$$word

б) P@ssw0rd

в) password

г) passw0rd

д) Password

1. Каким термином называется способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ? а) Линейное шифрование

б) Одноуровневое шифрование

в) Простое шифрование

г) Симметричное шифрование

д) "One-key" шифрование

1. Какой метод обмена ключами из перечисленных позволяет сторонам обменяться секретными ключами, не раскрывая их через незащищенную среду? а) Diffie-Hellman

б) Ceasar

в) Merkle-Hellman Knapsack

г) MD5

д) Twofish

1. Какой из следующих параметров веб-браузера необходимо использовать для настройки того, каким образом браузер получает информацию и загружает содержимое вебсайтов?

а) Cookies

б) Ничего из вышеперечисленного

в) Прокси-сервер

г) Сертификат

д) Безопасность

1. Вы получили по электронной почте письмо с вложением "От отдела IT". В тексте письма говорится, что ваш компьютер был заражен вирусом. Поэтому вам необходимо открыть вложение и следовать инструкциям, чтобы избавиться от вируса. Что необходимо сделать? (Выберите все подходящие варианты).

а) Связаться с IT-отделом для уточнения информации о полученном письме.

б) Откройте вложение, чтобы увидеть его содержание.

в) Следуйте инструкциям, чтобы удалить вирус.

г) Написать письмо отправителю с просьбой удалить из списка рассылки.

д) Удалить сообщение из неизвестного источника

1. На каком устройстве обычно используют технологию VLAN с целью разделения сети на сегменты? а) Брандмауер

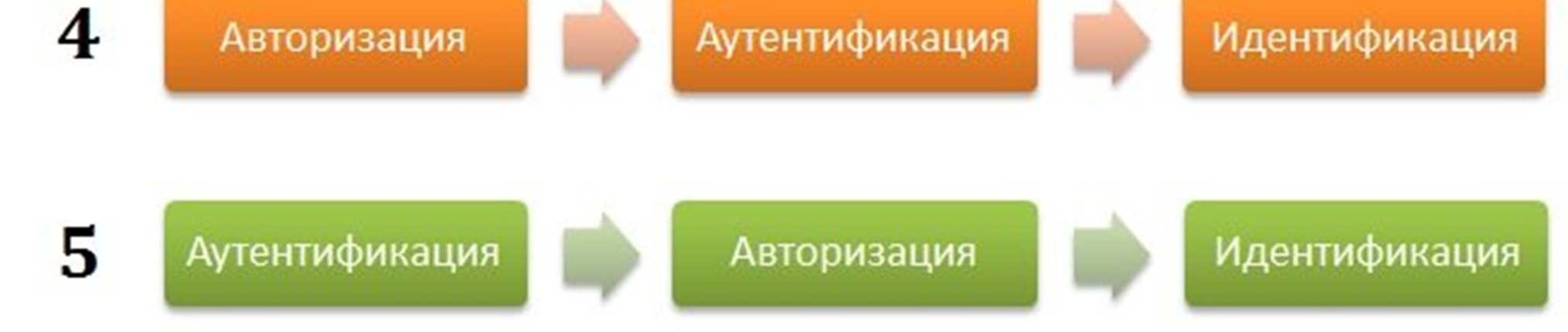
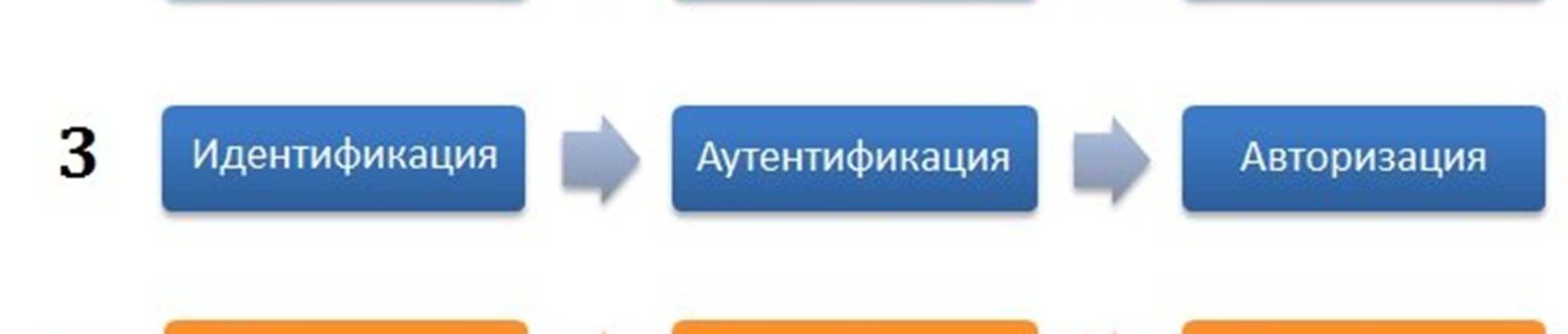
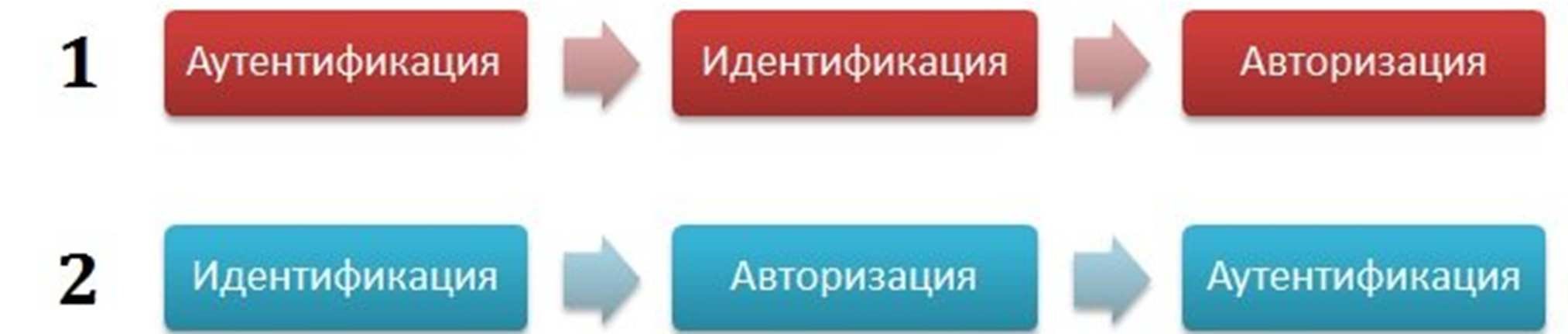
б) Точка доступа

в) Повторитель

г) Маршрутизатор

д) Коммутатор

1. Процесс регистрации пользователя в системе состоит из трёх взаимосвязанных, последовательно выполняемых процедур: ... (укажите их с учетом правильного порядка)



1. Какая из перечисленных технологий не относится к технологиям вероятностного анализа, применяемым в антивирусах? а) Анализ контрольных сумм

б) Сигнатурный анализ

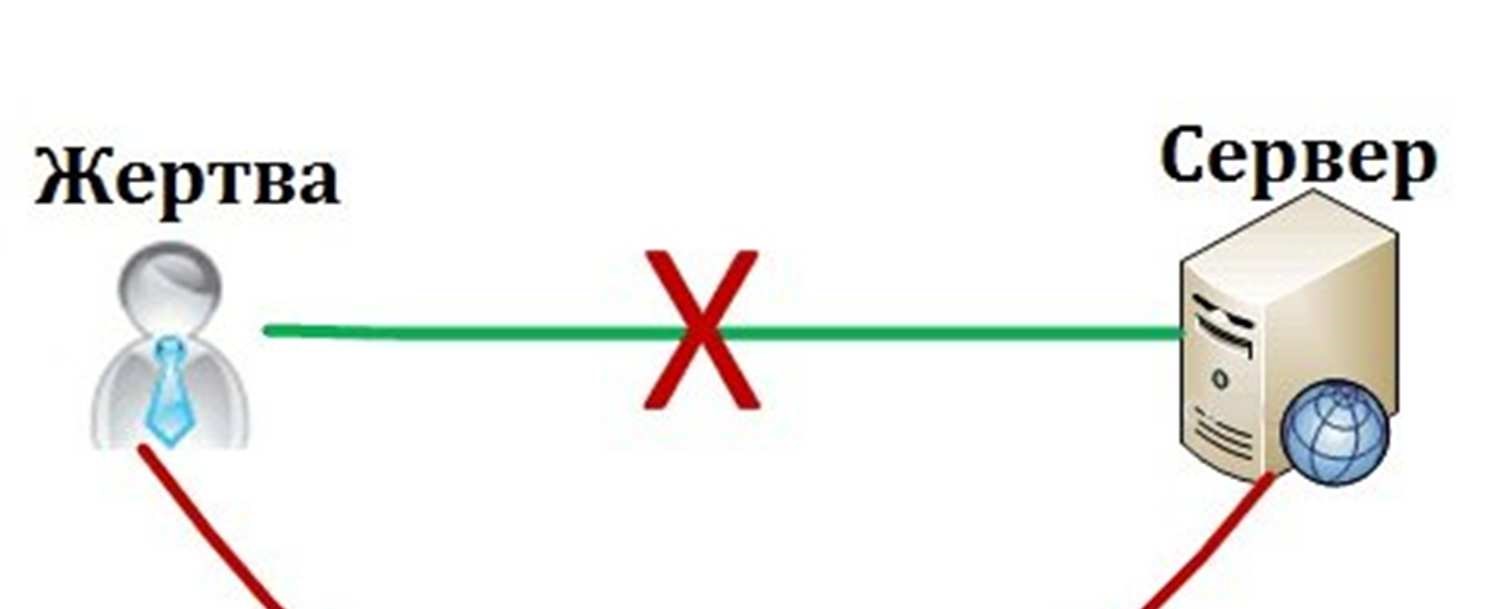
в) Нет верного ответа

г) Поведенческий анализ

д) Эвристический анализ

1. Определите название атаки, механизм которой обозначен на рисунке?

а) Buffer Overflow



б) Spoofing

в) DDoS

г) IP-spoofing

д) Man-in-the-Middle

1. Для чего не используются сканеры уязвимостей при аудите?

а) Для определения необходимых обновлений

б) Для выявления информации о небезопасном коде в приложениях

в) Для выявления открытых портов и сервисов, которые могут быть использованы хакерами для возможных атак

г) Для определения неверных (с точки зрения информационной безопасности) настроек системы

д) Для определения максимальной пропускной способности канала

1. Попытка реализации угрозы информационной безопасности - это... (выберите понятие в терминах информационной безопасности) а) Уязвимость

б) Атака

в) Нападение

г) Штурм

д) Контратака

1. На каком устройстве обычно используют технологию VLAN с целью разделения сети на сегменты? а) Брандмауер

б) Точка доступа

в) Повторитель

г) Маршрутизатор

д) Коммутатор

1. Какой трафик будет прослушивать нарушитель, если запустит пассивный снифинг пакетов?

а) Весь трафик сети



б) Весь трафик, идущий через маршрутизатор

в) Весь трафик VLAN 20

г) Только свой собственный

д) Весь трафик VLAN 10 и VLAN 20

Для ***продвинутого уровня*** он представляет собой тест на знания основных алгоритмов шифрования, получения ЭЦП, общих вопросов защиты информации, особенностей корректирующих кодов, методов безопасной передачи информации по каналам связи. Тест может содержать несколько верных ответов.

### *Фонд тестовых заданий*

1. Алгоритм RC6 обладает следующими свойствами

а) имеет самое быстрое установление ключа;

б) имеет самое быстрое шифрование/дешифрование;

в) имеет возможность вычисления подключей на лету;

г) шифрование и дешифрование имеют идентичные функции.

1. Алгоритм RSA может использоваться для

а) подписывания;

б) шифрования;

в)обмена общим секретом;

г) все выше перечисленное.

1. Алгоритм Serpent обладает следующими свойствами

а) имеет самое быстрое установление ключа;

б) имеет самое быстрое шифрование/дешифрование;

в) имеет возможность вычисления подключей на лету;

г) шифрование и дешифрование имеют идентичные функции.

1. В DSS используется следующая хэш-функция а) MD5;

б) SHA-1;

в) SHA-2;

г) нет верного ответа.

1. В алгоритме RC6 используются следующие операции а) XOR слов;

б) циклический сдвиг на несколько битов;

в) S-box;

г) нет верного ответа.

1. Выберите правильное высказывание

а) подпись с использованием эллиптических кривых является детерминированной;

б) подпись с использованием эллиптических кривых является рандомизированной;

в) уравнения на эллиптических кривых нельзя использовать для создания цифровых подписей; г) нет верного высказывания.

1. Выберите правильное утверждение

а) в основе алгоритма RС6 лежит традиционная сеть Фейштеля;

б) в основе алгоритма RС6 не лежит сеть Фейштеля;

в) в основе алгоритма RС6 лежит сеть Фейштеля смешанного типа с 4 ветвями; г) нет верного утверждения.

1. Выберите правильное утверждение

а) должно быть вычислительно невозможно подделать цифровую подпись как созданием нового сообщения для существующей цифровой подписи, так и созданием ложной цифровой подписи для некоторого сообщения; б) цифровая подпись должна быть достаточно компактной и не занимать много памяти;

в) подпись обязательно должна быть рандомизированной;

г) нет верного утверждения.

1. Выберите правильное утверждение:

а) в криптографии с использованием эллиптических кривых все значения вычисляются по модулю n, где n – произведение двух простых чисел;

б) в криптографии с использованием эллиптических кривых все значения вычисляются по модулю простого числа р;

в) в криптографии с использованием эллиптических кривых все значения вычисляются по модулю произвольного числа р

г) нет верного утверждения.

1. Выберите правильное утверждение:

а) в любом протоколе аутентификации ключ сессии всегда создается третьей доверенной стороной;

б) в любом протоколе аутентификации ключ сессии всегда создается участником А;

в) существуют различные протоколы, в одних ключ сессии создается KDC, в других - одним из участников А или

В;

г) нет верного утверждения.

1. Выберите правильное утверждение:

а) в протоколах аутентификации с использованием шифрования с открытым ключом участники должны знать открытый ключ AS или KDC;

б) в протоколах аутентификации с использованием шифрования с открытым ключом участники должны знать открытые ключи друг друга;

в) в протоколах аутентификации с использованием шифрования с открытым ключом участники должны знать как открытый ключ AS или KDC, так и открытые ключи друг друга; г) нет верного утверждения.

1. Выберите правильное утверждение:

а) в основе алгоритма DES лежит сеть Фейштеля;

б) в алгоритме DES используются S-boxes;

в) в алгоритме DES используется умножение по модулю 216 + 1;

г) нет верного утверждения.

1. Выберите правильное утверждение:

а) подпись должна быть битовым образцом, который зависит от подписываемого сообщения;

б) подпись должна использовать некоторую уникальную информацию отправителя для предотвращения подделки или отказа;

в) подпись должна обеспечивать невозможность просмотра сообщения;

г) нет верного утверждения.

1. Выберите правильные утверждения:

а) должно быть относительно легко создавать цифровую подпись;

б) должно быть относительно трудно создавать цифровую подпись;

в) должно быть относительно легко проверять цифровую подпись;

г) нет верного утверждения.

1. Выберите правильное утверждение:

а) мастер-ключ должен быть более защищенным, чем ключ сессии+++++;

б) ключ сессии должен быть более защищенным, чем мастер-ключ;

в) мастер-ключ и ключ сессии должны иметь одинаковую степень защиты;

г) нет верного утверждения.

1. Выходом хэш-функции является:

а) сообщение той же длины, что и входное сообщение;

б) сообщение фиксированной длины;

в) сообщение меньшей длины;

г) нет верного ответа.

1. Длина блоков, на которые делится сообщение в хэш-функции SHA-1, равна: а) 160 бит;

б) 512 бит;

в) 1024 бит;

г) нет верного ответа.

1. Длина блоков, на которые делится сообщение в хэш-функции SHA-512, равна: а) 512 бит;

б) 1024 бит;

в) 1024 байт;

г) нет верного ответа.

1. Длина блоков, на которые делится сообщение в хэш-функции ГОСТ 3411, равна: а) 256 бит;

б) 512 бит;

в) 1024 бит;

г) нет верного ответа.

1. Длина ключа в алгоритме ГОСТ 28147: а) 56 бит;

б) 128 бит;

в) 256 бит;

г) 448 бит.

1. Длина хэш-кода, создаваемого хэш-функцией SHA-1, равна: а) 128 бит;

б) 160 бит;

в) 512 бит;

г) 1024 бит.

1. Дополнительными параметрами хэш-функции ГОСТ 3411 являются: а) стартовый вектор хэширования;

б) ключи для алгоритма симметричного шифрования ГОСТ 28147;

г) начальное значение хэш-кода;

г) нет верного ответа.

1. Каждый блок сообщения в хэш-функции MD5 обрабатывается: а) 4 раза;

б) 16 раз;

в) 64 раза;

г) 128 раз.

1. Из двух компонент (r, s) состоит подпись, полученная с использованием алгоритма: а) RSA;

б) DSS;

в) ГОСТ 3410;

г) нет верного ответа.

1. Зависимость между ключами шифрования и дешифрования в алгоритмах симметричного шифрования должна быть следующей:

а) ключи шифрования и дешифрования должны в точности совпадать;

б) ключ дешифрования должен легко получаться из ключа шифрования;

в) между ключами шифрования и дешифрования не должно быть никакой зависимости; г) нет верного ответа.

1. Криптографическая система называется симметричной, потому что:

а) шифруемый блок разбивается на подблоки одинаковой длины;

б) для шифрования и дешифрования используются одинаковые или легко выводимые один из другого ключи;

г) алгоритм использует циклически повторяющиеся операции, называемые раундами; г) нет верного ответа.

1. Криптография с использованием эллиптических кривых дает преимущества по сравнению с другими алгоритмами, потому что: а) принципиально не может быть взломана;

б) обеспечивает эквивалентную защиту при меньшей длине ключа;

г) проще в реализации;

г) нет верного ответа.

1. Нулевым элементом эллиптической кривой считается точка О, которая: а) имеет координаты (0, 0);

б) является бесконечно удаленной точкой, в которой сходятся все вертикальные прямые; в) имеет координаты (0, 1) или (1, 0);

г) нет верного ответа.

1. Побитовый XOR блоков нельзя считать криптографической хэш-функцией, потому что:

а) противник может легко подобрать другое сообщение, имеющее тот же хэш-код;

б) побитовый XOR плохо защищает от случайного сбоя;

в) побитовый XOR требует сложных вычислений;

г) нет верного ответа.

1. Под DoS-атакой понимается:

а) модификация передаваемого сообщения;

б) повторное использование переданного ранее сообщения;

в) невозможность получения сервиса законным пользователем;

г) нет верного ответа.

1. Под replay-атакой понимается:

а) модификация передаваемого сообщения;

б) повторное использование переданного ранее сообщения;

в) невозможность получения сервиса законным пользователем;

г) нет верного ответа.

1. Подпись называется детерминированной, если:

а) для одного и того же сообщения с использованием разных закрытых ключей при каждом подписывании создается одна и та же подпись;

б) для разных сообщений с использованием одного и того закрытого ключа при каждом подписывании создается одна и та же подпись;

в) для одного и того же сообщения с использованием одного и того же закрытого ключа при каждом подписывании создается одна и та же подпись;

г) нет верного ответа.

1. При использовании криптографии на эллиптических кривых в качестве аналога алгоритма Диффи-Хеллмана в уравнении PA = nA×G:

а) открытым ключом участника А является PA, закрытым ключом участника А является nA;

б) открытым ключом участника А является nA, закрытым ключом участника А является PA;

в) открытым ключом участника А является PA, закрытым ключом участника А является G; г) нет верного ответа.

1. При односторонней аутентификации ключ сессии может шифроваться: а) открытым ключом получателя;

б) закрытым ключом отправителя;

в) мастер-ключом для симметричного шифрования, разделяемым отправителем и KDC; г) нет верного ответа.

1. Причина использования двух ключей в тройном DES состоит в том, что:

а) в этом случае отсутствует атака «встреча посередине»;

б) стойкость алгоритма не повышается при использовании трех ключей вместо двух;

в) при использовании трех ключей общая длина ключа равна 168 битам, что может потребовать существенно больших вычислений при его распределении; г) нет верного ответа.

1. Сервис, который гарантирует, что информация получена из законного источника и получателем является тот, кто нужно, называется: а) аутентификацией;

б) целостностью;

в) конфиденциальностью;

г) нет верного ответа.

1. Сервис, который обеспечивает невозможность несанкционированного просмотра данных, называется: а) аутентификацией;

б) целостностью;

в) конфиденциальностью;

г) нет верного ответа.

1. Хэш-функции предназначены для:

а) сжатия сообщения;

б) получения «отпечатков пальцев» сообщения;

в) шифрования сообщения;

г) нет верного ответа.

1. Хэш-функция должна обладать следующими свойствами:

а) хэш-функция должна применяться к блоку данных любой длины;

б) хэш-функция должна создавать выход произвольной длины;

в) для любого данного значения хэш-кода h вычислительно невозможно найти M такое, что Н (M) = h; г) нет верного ответа.

1. Шифрование/дешифрование с использованием эллиптических кривых выполняется следующим образом:

а) участник А выбирает случайное целое положительное число k и вычисляет зашифрованное сообщение Cm, являющееся точкой на эллиптической кривой Cm = {k ×G, Pm + k ×PB};

б) участник А выбирает случайное целое положительное число k и вычисляет зашифрованное сообщение Cm, являющееся точкой на эллиптической кривой Cm = { Pm + k ×PB};

в) участник А выбирает случайное целое положительное число k и вычисляет зашифрованное сообщение Cm, являющееся точкой на эллиптической кривой Cm = {k ×G}; г) нет верного ответа.

Для ***высокого уровня*** он представляет собой контрольные задания на знания основных алгоритмов шифрования, получения ЭЦП, общих вопросов защиты информации, особенностей корректирующих кодов, методов безопасной передачи информации по каналам связи. Тест не содержит вариантов ответов. Ответы должны быть сформулированы кратко и аргументировано.

### *Комплект контрольных заданий*

1. Персоналу в случае возникновения нештатной ситуации необходимо иметь:
2. Повторное использование переданного ранее сообщения называется …
3. Политика безопасности – это …
4. Политика информационной безопасности в общем случае является руководящим документом для …
5. Политика информационной безопасности, прежде всего, необходима для …
6. Пользователь осуществляет удаленный доступ к информации на сервере. Пусть условный уровень защищенности информации на сервере - 24 единицы; условный уровень защищенности рабочего места пользователя - 10 единиц. Оцените условный уровень защищенности удаленного доступа пользователя к информации на сервере.
7. Пороговый метод выявления атак хорош тем, что …
8. После идентификации угрозы необходимо оценить …
9. Правило, которым необходимо пользоваться при формировании матрицы доступа …
10. Предположим, информационная система компании надежно защищена комплексом средств информационной защиты (межсетевые экраны, антивирусы, системы защиты от НСД, системы обнаружения атак и т.д.). Как на существующий уровень рисков влияет реализация требований политики безопасности?
11. При внесении изменений в систему требуется …
12. При выведении из эксплуатации устройств хранения информации необходимо …
13. При использовании версии сервера аутентификации Kerberos, описанной в курсе, шифрование …
14. При односторонней аутентификации осуществляется аутентификация …
15. Применение метода разделения обязанностей необходимо для …
16. Принцип усиления самого слабого звена можно переформулировать как принцип …
17. Протоколирование и аудит могут использоваться для …
18. Процедура входа в систему (login) не должна выдавать …
19. Пункт, в котором перечислено наибольшее число событий, которые рекомендуется фиксировать в журнале данных о доступе …
20. Пункт, точно соответствующий рекомендованным стандартом ограничениям на использование системных утилит…
21. Согласно "Оранжевой книге", политика безопасности включает в себя следующие элементы …
22. Согласно рекомендациям X.800, аутентификация не может быть реализована на …
23. Согласно стандарту X.700, в число функций управления конфигурацией входят …
24. Специальные соглашения, необходимые при приеме персонала на работу о(об) …
25. Список открытых портов, наиболее свойственный для системы Windows 9x …
26. Стандарт, широко признанный как стандарт лучшей практики защиты …
27. Тип межсетевого экрана, который может контролировать выполнение команды PUT сервиса FTP и фильтровать теги HTTP …
28. Требование односторонности хэш-функции состоит в следующем …
29. Туннелирование может применяться для достижения следующих целей …
30. Формируя привилегии индивидуальных пользователей, выдаваемым по мере необходимости, следует пользоваться принципом наделения пользователей …
31. Функция, используемая в криптосистеме с открытым ключом, должна обладать следующими свойствами …
32. Цифровой сертификат содержит ЭЦП …
33. Чтобы узнать открытые порты на своем компьютере, необходимо выполнить команду …
34. Алгоритм симметричного шифрования называется блочным, если…
35. Международный стандарт управления информационной безопасностью ISO 17799 предъявляет …

### 3.2.2. Практические занятия

Данный вид контроля за учебной деятельностью студентов осуществляется в течение семестра. Посещение практических занятий и выполнения заданий является допуском к зачёту (промежуточной аттестации) по дисциплине. Студент не допускается к экзамену (промежуточной аттестации), если не сданы тесты и контрольные работы по всем учебным модулям, а также в случае не добора баллов согласно бально-рейтинговой системы (менее 35).

### 3.2.3. Лабораторные занятия

Данный вид контроля за учебной деятельностью студентов осуществляется в течение семестра. Посещение лабораторных занятий и выполнения заданий является допуском к зачёту (промежуточной аттестации) по дисциплине. Студент не допускается к экзамену (промежуточной аттестации), если не сданы тесты и контрольные работы по всем учебным модулям, а также в случае не добора баллов согласно бально-рейтинговой системы (менее 35).

Баллы за каждый учебный модуль суммарно складываются из количества баллов, набранных в ходе текущего контроля, проводимого на лабораторных и практических занятиях (максимальное количество – 5 баллов), и количества баллов, полученных за выполнение заданий **на практических и лабораторных занятиях** (1УМ – 5 баллов, 2УМ – 9 баллов, 3УМ – 11 баллов, 4УМ – 15 баллов).

#### 3.3. Экзамен (промежуточная аттестация) по дисциплине

Экзамен является итоговой формой оценки знаний студентов, приобретённых в течение обучения по дисциплине. Экзамен проводится в устной форме (обучающийся тезисно пишет ответ на вопросы) с дальнейшим собеседованием по вопросам из билета. Студент выбирает билет, содержащий 3 вопроса из базового и продвинутого уровня, вопросы высокого уровня задаются дополнительно (устно при собеседовании). Билеты формируются преподавателем перед зачетно-экзаменационной сессией.

По результатам ответов на промежуточной аттестации выставляется максимально 40 баллов: при полном ответе на вопрос базового уровня – 10 баллов, базового и продвинутого – 25 баллов; базового, продвинутого и высокого – 40 баллов. В случае неполных ответов по билету или спорной оценки задаются дополнительные вопросы из общего списка (вне зависимости от уровня освоения) по усмотрению преподавателя.

Итоговая оценка по дисциплине представляет собой сумму из баллов полученных в течении семестра и баллов полученных на промежуточной аттестации.

#### Шкала оценивания результатов

|  |  |
| --- | --- |
| Оценка | Баллы |
| удовлетворительно | 55-75 |
| хорошо | 76-90 |
| отлично | 91-100 |

***Вопросы для подготовки к экзамену***

#### Вопросы для базового уровня

1. Основные понятия информационной безопасности и защиты информации
2. Угрозы информационной безопасности
3. Угрозы и уязвимости беспроводных сетей
4. Основные понятия политики безопасности
5. Структура политики безопасности организации
6. Роль стандартов информационной безопасности
7. Симметричные криптосистемы шифрования
8. Основные режимы работы блочного симметричного алгоритма
9. Особенности применения алгоритмов симметричного шифрования
10. Асимметричные криптосистемы шифрования
11. Функции хэширования
12. Электронная цифровая подпись
13. Управление криптоключами
14. Аутентификация, авторизация и администрирование действий пользователей
15. Комбинированные системы идентификации и аутентификации

#### Вопросы для продвинутого уровня

1. Основные понятия информационной безопасности и защиты информации
2. Угрозы информационной безопасности
3. Характерные особенности сетевых атак
4. Угрозы и уязвимости беспроводных сетей
5. Обеспечение информационной безопасности компьютерных систем
6. Основные понятия политики безопасности
7. Структура политики безопасности организации
8. Разработка политики безопасности организации
9. Роль стандартов информационной безопасности
10. Международные стандарты информационной безопасности
11. Отечественные стандарты безопасности информационных технологий
12. Основные понятия криптографической защиты информации
13. Симметричные криптосистемы шифрования
14. Алгоритмы шифрования DES и 3-DES
15. Стандарт шифрования ГОСТ 28147-89: суть, режимы работы
16. Стандарт шифрования AES
17. Основные режимы работы блочного симметричного алгоритма
18. Особенности применения алгоритмов симметричного шифрования
19. Асимметричные криптосистемы шифрования
20. Алгоритм шифрования RSA
21. Ассиметричные криптосистемы на базе эллиптических кривых. Алгоритм ассиметричного шифрования ECES
22. Функции хэширования. Отечественный стандарт хэширования ГОСТ Р34.11-94
23. Электронная цифровая подпись. Основные процедуры цифровой подписи,
24. Алгоритм цифровой подписи DSA. Алгоритм цифровой подписи ECDSA
25. Алгоритм цифровой подписи ГОСТ Р 34.10-94. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-2001
26. Управление криптоключами: использование комбинированной криптосистемы, метод распределения ключей Диффи-Хеллмана
27. Инфраструктура управления открытыми ключами PKI: принцип функционирования

PKI, логическая структура и компоненты PKI

1. Аутентификация, авторизация и администрирование действий пользователей
2. Методы аутентификации, использующие пароли: аутентификация на основе многоразовых паролей, аутентификация на основе одноразовых паролей
3. Строгая аутентификация: основные понятия, применение электронных идентификаторов
4. Криптографические протоколы строгой аутентификации
5. Биометрическая аутентификация пользователя: дактилоскопические системы аутентификации, системы аутентификации по лицу и голосу, системы аутентификации по узору радужной оболочки и сетчатки глаз, области применения биометрических систем, биометрические идентификаторы
6. Комбинированные системы идентификации и аутентификации: радиочастотные идентификаторы и USB-ключи, гибридные смарт-карты, биоэлектронные системы. Электронные замки
7. Управление доступом по схеме однократного входа с авторизацией Single Sign-On:

простая система однократного входа Single Sing-On, системы однократного входа Web SSO,

SSO-продукты уровня предприятия

1. Управление идентификацией и доступом
2. Вредоносные программы и проблемы антивирусной защиты: компьютерные вирусы, жизненный цикл вирусов, сетевые черви, троянские программы, другие вредоносные программы и нежелательная корреспонденция
3. Основные каналы распространения вредоносных программ
4. Антивирусные программы: основы работы антивирусных программ, особенности «облачной» антивирусной технологии, виды антивирусных программ, дополнительные модули антивирусных программ, режимы работы антивируса
5. Профилактические меры защиты
6. Дополнительные средства защиты: обновления ПО, брандмауэры, средства защиты от нежелательной корреспонденции
7. Антивирусные программные комплексы: антивирус Касперского (АVР), антивирус Dr. Web, антивирус Norton AntiVirus от Symantec, антивирус McAfee, антивирус AntiVir Personal Edition

#### Вопросы для высокого уровня

1. Сформулируйте понятие информационной безопасности ИС.
2. Объясните понятия целостности, конфиденциальности и доступности информации.
3. Укажите отличия санкционированного доступа к информации от несанкционированного.
4. Перечислите основные признаки классификации возможных угроз безопасности ИС
5. Дайте краткую характеристику угрозы безопасности, обозначаемой термином «троянский конь».
6. Дайте краткую характеристику угроз безопасности, обозначаемых терминами «вирус» и «червь».
7. Назовите и охарактеризуйте наиболее распространенные виды сетевых.
8. Опишите атаку «человек-в-середине». Какие средства позволяют эффективно бороться с атаками такого типа?
9. Опишите атаку типа «отказ в обслуживании» и распределенную атаку «отказ в обслуживании».
10. Опишите особенности фишинга и фарминга. Укажите меры противодействия этим атакам.
11. Каковы источники нарушений безопасности проводных корпоративных сетей?
12. Назовите основные уязвимости и угрозы беспроводных сетей.
13. Объясните понятие «политика безопасности организации».
14. Какие разделы должна содержать документально оформленная политика безопасности?
15. Какие проблемы решает верхний уровень политики безопасности?
16. Какие задачи решает средний уровень политики безопасности?
17. Каковы особенности нижнего уровня политики безопасности?
18. Сформулируйте обязанности руководителей подразделений, администраторов и пользователей при реализации политики безопасности.
19. Опишите структуру политики безопасности организации.
20. Что представляют собой специализированные политики безопасности?
21. Приведите несколько примеров специализированных политик безопасности с описанием их особенностей.
22. Что представляют собой процедуры безопасности?
23. Приведите несколько примеров процедур безопасности с описанием их особенностей.
24. Перечислите основные этапы разработки политики безопасности организации.
25. Сформулируйте главную задачу стандартов информационной безопасности с позиций производителен и потребителей продуктов информационных технологий, а также специалистов по сертификации этих продуктов.
26. Назовите основные международные стандарты информационной безопасности.
27. Дайте краткую характеристику международного стандарта IS0/IEC 17799:2000 (BS 7799-1:2000).
28. Каковы основные особенности германского стандарта BSI «Руководство но защите информационных технологий для базового уровня защищенности»?
29. Опишите содержание и укажите значение международного стандарта ISO 15408 «Общие критерии безопасности информационных технологий».
30. Перечислите стандарты для беспроводных сетей и дайте их краткую характеристику.
31. Назовите стандарты информационной безопасности для Интернета.
32. Каковы назначение и особенности функционирования протокола SET?
33. Каковы назначение и функциональность протоколов SSL и IPSec? В чем эти протоколы существенно различаются?
34. Каковы назначение и функциональность инфраструктуры управления открытыми ключами PKI?
35. Перечислите российские стандарты безопасности информационных технологий.
36. Каково назначение стандарта ГОСТ Р ИСО/МЭК 15408? Назовите и охарактеризуйте три основных части этого стандарта.
37. Что такое криптография?
38. Дайте определения следующих понятий: криптограмма, криптоалгоритм, криптосистема 39. В чем состоит коренное различие симметричных и асимметричных криптосистем?
39. Охарактеризуйте четыре основных режима работы блочного алгоритма.
40. Расскажите о способах комбинирования блочных алгоритмов для получения алгоритмов с более длинным ключом, сравните их между собой.
41. Каковы основные характеристики и режимы работы отечественного стандарта шифрования данных?
42. Сформулируйте концепцию криптосистемы с открытым ключом.
43. Дайте определение однонаправленной функции. Приведите примеры однонаправленных функций
44. Каковы особенности однонаправленных функций с секретом?
45. На чем основывается надежность криптоалгоритма шифрования RSA?
46. Опишите две основные процедуры, осуществляемые системой электронной цифровой подписи для подтверждения подлинности цифрового документа.
47. Опишите отечественный стандарт цифровой подписи, укажите его преимущество по сравнению с алгоритмом цифровой подписи DSA.
48. Каково назначение хэш-функция и каким требованиям должна удовлетворять качественная хэш-функция?
49. Каким образом комбинированный метод шифрования позволяет сочетать достоинства ассиметричных и симметричных криптосистем? Опишите протокол реализации комбинированного метода шифрования.
50. Опишите работу алгоритма Диффи-Хэллмана. Укажите достоинства этого алгоритма.
51. Каково назначение инфраструктуры открытых ключей PKI? Опишите функционирование инфраструктуры PKI.
52. Дайте определение понятий «идентификация», «аутентификация», «авторизация», «администрирование».
53. Что понимают под решением задач ААА?
54. Какие задачи решает подсистема управления идентификацией и доступом IAM?
55. На какие категории можно разделить процессы аутентификации в зависимости от сущностей, предъявляемых пользователем для подтверждения своей подлинности?
56. Перечислите основные атаки на протоколы аутентификации.
57. Опишите метод аутентификации на основе многоразовых паролей. Каковы его недостатки?
58. Опишите метод аутентификации на основе одноразовых паролей. Каковы его достоинства и недостатки?
59. Сформулируйте принцип строгой аутентификации. Опишите типы процедур строгой аутентификации.
60. Объясните назначение PIN-кода и особенности его использования.
61. Объясните принцип работы двухфакторной аутентификации. Какие внешние носители информации используют для двухфакторной аутентификации пользователей? Каковы достоинства этого метода аутентификации?
62. Опишите функциональность и характеристики смарт-карт и USB-токенов.
63. Опишите методы биометрической аутентификации пользователя.

64.Что означают термины «коэффициент ошибочных отказов» и «коэффициент ошибочных подтверждений»?

65.Объясните принцип управления доступом но схеме однократного входа с авторизацией SSO.

1. Что такое вредоносная программа? Охарактеризуйте основные типы вредоносных программ.
2. Укажите существенные отличия компьютерных вирусов от сетевых червей. Опишете основные особенности троянских программ.
3. Опишите два основных подхода к обнаружению вредоносных программ.
4. Как выполняется сигнатурный анализ? Каковы его достоинства и недостатки?
5. Что представляют собой проактивные методы обнаружения? Дайте характеристики двух наиболее популярных подходов.
6. Опишите принцип действия, достоинства и недостатки эвристических анализаторов.
7. Опишите принцип действия, достоинства и недостатки поведенческих блокираторов.
8. Назовите и опишите дополнительные модули антивирусных средств.
9. Каковы дополнительные меры и средства защиты от вредоносных программ, расширяющие возможности антивирусных программ?
10. Опишите меры и средства зашиты от спама.
11. Каковы особенности реализации подсистемы защиты корпоративной информации от вредоносных программ и вирусов?
12. Каковы возможности серии продуктов Kaspersky Open Space Security для зашиты корпоративных сетей от современных интернет-угроз?

Разработанные контролирующие материалы позволяют оценить степень усвоения теоретических и практических знаний, приобретенные умения и владение опытом на репродуктивном уровне, когнитивные умения на продуктивном уровне, и способствуют формированию профессиональных и общекультурных компетенций студентов, что является очень важным в деле подготовки высококвалифицированных бакалавров по направлению 09.03.01 «Информатика и вычислительная техника» профиля подготовки «Технологии разработки программного обеспечения».

\* \* \*

Фонд оценочных средств по дисциплине Б3.Б.8 «Информационная безопасность» разработан в соответствии с требованиями ФГОС ВПО, с учетом рекомендаций ПрООП ВПО образовательной программы «Прикладная информатика в экономике» по направлению подготовки бакалавров 09.03.03. «Прикладная информатика».

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ к. т. н., доцент Косулин В.В.

Автор (подпись, дата)

Фонд оценочных средств обсужден и одобрен на заседании кафедры ИИУС от 15.05.2017 г., протокол № 5.

Зав. кафедрой ИИУС \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ к. т. н., доцент Косулин В.В.

(подпись, дата)

На заседании методического совета института ИЭИТ 20.05.2017 г., протокол № 21 фонд оценочных средств рекомендован к утверждению.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Директор ИЭИТ (подпись, дата) к. ф.-м. н., доцент Смирнов Ю.Н.

Эксперты:

Главный специалист отдела \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Салтанаев Э.И.

информационных технологий (подпись, дата)

ГАУЗ РКБ № 2