**Тамбовское государственное автономное профессиональное**

**образовательное учреждение «Тамбовский бизнес-колледж»**

**Предметно-цикловая комиссия информационных технологий**

Утверждаю:

Директор ТОГАПОУ

«Тамбовский бизнес-колледж»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Н.В. Астахова

«28» августа 2017 г.

**Фонд оценочных средств**

текущего контроля и промежуточной аттестации по учебной дисциплине

**ОП.15 Защищенный документооборот**

среднее профессиональное образование

(программа подготовки специалистов среднего звена)

**10.02.05 «Обеспечение информационной безопасности автоматизированных систем»**

Тамбов 2017

**Лист согласования**

**программы фонда оценочных средств учебной дисциплины**

**ОП.15 «Защищенный документооборот»**

Рабочая программа является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Информатика и вычислительная техника, в части освоения основного вида профессиональной деятельности: обработка отраслевой информации изучаемой в учреждениях среднего профессионального образования при подготовке квалифицированных специалистов среднего звена.

**Организация разработчик:**

Тамбовское областное государственное автономное профессиональное образовательное учреждение «Тамбовский бизнес-колледж»

**Разработчики:**

Трефилов П.А. - преподаватель ТОГАПОУ «Тамбовский бизнес-колледж».

Программа рассмотрена и рекомендована ПЦК информационных технологий ТОГАПОУ «Тамбовский бизнес-колледж» Протокол № 1 от «28» августа 2017 г.

|  |
| --- |
| СОГЛАСОВАНО:  АНО «Академический правовой центр»  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ О.В. Штах  «28» августа 2017 г. |

**АННОТАЦИЯ**

**программы фонда оценочных средств учебной дисциплины**

ОП.15 Защищенный документооборот

ФОС является составной частью образовательной программы - ППССЗ по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем и предназначен для оценки качества подготовки обучающихся и выпускников ППССЗ по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем. Объектами оценки являются знания, умения и практический опыт как элементы общих и профессиональных компетенций.

В результате освоения дисциплины обучающийся должен:

**уметь:**

- отыскивать необходимые нормативные правовые акты и информационные правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации;

- применять действующую законодательную базу в области информационной безопасности;

- разрабатывать проекты положений, инструкций и других организационно-распорядительных документов, регламентирующих работу по защите информации.

**знать:**

- содержание основных понятий обеспечения информационной безопасности;

- источники угроз безопасности информации;

- методы оценки уязвимости информации;

- методы создания, организации и обеспечения функционирования систем комплексной защиты информации;

- методы пресечения разглашения конфиденциальной информации;

- виды и признаки компьютерных преступлений.

В результате освоения дисциплины формируются компетенции:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6 Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7 Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.

ОК 8 Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.

ПК 2.1 Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами

ПК 2.4 Осуществлять обработку, хранение и передачу информации ограниченного доступа

Использование фонда оценочных средств направлено на достижение общеобразовательных, воспитательных и практических задач, на дальнейшее развитие личностных способностей и дальнейшего профессионального роста выпускника – будущего специалиста.

**СОДЕРЖАНИЕ**

|  |  |
| --- | --- |
|  | Стр. |
| 1. Паспорт фонда оценочных средств | 6 |
| 1.1. Область применения | 6 |
| 1.1.1 Карта компетенций | 6 |
| Показатели оценивания планируемых результатов обучения | 9 |
| 2. Контроль и оценка освоения теоретического и практического курса учебной дисциплины «Защищенный документооборот» | 9 |
| 2.1. Общие положения освоения учебной дисциплины по темам | 9 |
| 2.2. Задания для оценки освоения теоретического и практического курса учебной дисциплины | 9 |
| 3. Материалы для промежуточной аттестации по учебной дисциплине | 36 |
| 4. Критерии оценки | 39 |
| 5. Список рекомендуемой литературы. | 40 |

**1. Паспорт фонда оценочных средств**

**1.1. Область применения**

Комплект фонда оценочных средств предназначен для проверки результатов освоения учебной дисциплины ОП15 «Защищенные документооборот» программы подготовки специалистов среднего звена по специальности СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

**1.1.1 Карта компетенций**

Таблица 1

|  |  |
| --- | --- |
| Контролируемые компетенции (шифр компетенции) | Планируемые результаты обучения (знает, умеет, владеет, имеет навык) |
| ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес. | **Знать:** возможности трудоустройства и варианты построения трудовой карьеры на базе профессии обучения; видов и типов предприятий, форм занятости для трудоустройства по профессии обучения |
| **Уметь:** обосновывать выбор своей будущей профессии, ее преимущества и значимость на современном рынке труда России |
| **Владеть:** возможностями использования умений и навыков, приобретенных в ходе изучения учебного курса (дисциплины), в будущей профессионально-трудовой деятельности |
| ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество | **Знать:** виды и типы проблем в профессиональной деятельности, обобщенные способы их разрешения; типов и видов планирования работ, построения планов-графиков профессиональной деятельности; возможности повышения профессиональной квалификации |
| **Уметь:** планировать профессиональную деятельность, самообразование и организовывать их выполнение в соответствии с планом; выбирать эффективный способ решения проблем при наличии альтернативы и обосновывать его |
| **Владеть:** практическим опытом планирования работ, исходя из целей и задач деятельности, определенных руководителем; выбора средств реализации целей и задач, поставленных руководителем |
| ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личного развития | **Знать:** типы и виды источников информации в профессиональной области, их особенности и способы получения, способов работы с информацией при разрешении профессионально-трудовых проблем. |
| **Уметь:** осуществлять поиск, обработку и представление информации в различных форматах (таблицы, графики, диаграммы, текст и т.д.), в том числе – с использованием компьютерных программ; выделять существенное содержание в технических инструкциях и регламентах |
| **Владеть:** практическим опыта самостоятельного поиска информации из различных источников (в том числе – профессиональных изданий, Интернета и т.д.), необходимой для решения профессионально- трудовых задач; обработки и представления информации в различных форматах для разных групп пользователей (в том числе – администрации, коллег, клиентов и т.д.) |
| ОК 5. Владеть информационной культурой, анализировать и оценивать информацию с использованием информационно-коммуникативных технологий | **Знать:** основы работы с текстовыми редакторами, электронными таблицами, электронной почтой, мультимедийным оборудованием; способов работы с информацией при разрешении профессионально-трудовых проблем. |
| **Уметь:** осуществлять поиск, обработку и представление информации в различных форматах, с использованием компьютерных программ; (электронные таблицы, графики, диаграммы, текст и т.д.) |
| **Владеть:** практическим опытом самостоятельного поиска информации с использованием информационно-коммуникационных технологий, необходимой для решения профессионально-трудовых задач; обработки и представления информации в различных форматах для разных групп пользователей (в том числе – администрации, коллег, клиентов и т.д.) |
| ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями. | **Знать:** основные профессиональные технические термины и определения профессиональной области |
| **Уметь:** грамотно разъясняться с коллегами на профессиональные темы; сформулировать задачу |
| **Владеть:** практическим опытом коллективного решения задач в профессиональной области |
| ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. | **Знать:** ответственность за работу членов команды (подчиненных), результат выполнения заданий |
| **Уметь:** нести ответственность за работу членов команды (подчиненных), результат выполнения заданий |
| **Владеть:** практическим опытом несенияответственности за работу членов команды (подчиненных), результат выполнения заданий |
| ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации. | **Знать:** принципы определения задачи профессионального и личностного развития |
| **Уметь:** самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации. |
| **Владеть:** навыками самостоятельного определения задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации. |
| ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности. | **Знать:** основополагающие принципы функционирования технологий в профессиональной деятельности |
| **Уметь:** ориентироваться в условиях частой смены технологий в профессиональной деятельности |
| **Владеть:** навыками самостоятельного освоения новых методов и технологий в профессиональной деятельности |
| ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках. | **Знать:** уметь пользоваться профессиональной документацией на государственном и иностранном языках. |
| **Уметь:** Пользоваться профессиональной документацией на государственном и иностранном языках. |
| **Владеть:** Навыками пользования профессиональной документацией на государственном и иностранном языках |
| ПК 2.1 Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами | **Знать:** методы обеспечения защиты информации в автоматизированных системах отдельными программами, программно-аппаратными средствами |
| **Уметь:** Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами |
| **Владеть:** навыками обеспечения защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами |
| ПК 2.4 Осуществлять обработку, хранение и передачу информации ограниченного доступа | **Знать:** способы осуществления обработки, хранения и передачи информации ограниченного доступа |
| **Уметь:** Осуществлять обработку, хранение и передачу информации ограниченного доступа |
| **Владеть:** приемами осуществления обработки, хранения и передачи информации ограниченного доступа |

1.1.2 Показатели оценивания планируемых результатов обучения

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Семестр | Шкала оценивания | | | |
| 2 | 3 | 4 | 5 |
| 7 семестр | ОК1-ОК10 | ОК1-ОК10, ПК2.1 ПК2.4 | ОК1-ОК10, ПК2.1 ПК2.4 | ОК1-ОК10, ПК2.1 ПК2.4 |
| 8 семестр | ОК1-ОК10 | ОК1-ОК10, ПК2.1 ПК2.4 | ОК1-ОК10, ПК2.1 ПК2.4 | ОК1-ОК10, ПК2.1 ПК2.4 |

**2. Контроль и оценка освоения теоретического и практического курса учебной дисциплины «Защищенный документооборот»**

**2.1. Общие положения освоения учебной дисциплины по темам**

Основной целью оценки учебной дисциплины ОП.06 «Защищенный документооборот» является оценка знаний и умений.

Оценка теоретического, практического курса учебной дисциплины ОП.15 «Защищенный документооборот» осуществляется с использованием следующих форм и методов контроля: индивидуального и фронтального опроса, выполнения ситуационных заданий, тестирования.

**2.2. Задания для оценки освоения теоретического и практического** **курса учебной дисциплины:**

В процессе домашней подготовки к занятиям по соответствующей теме студенты должны:

- изучить конспект лекции;

- изучить рекомендованные по соответствующей теме учебники, учебные пособия, а также по своему усмотрению выбрать дополнительную литературу;

- подготовить ответы на вопросы, сформулированные в задании.

**3. Материалы для промежуточной аттестации по учебной дисциплине**

**Примеры типовых тестовых заданий (6 семестр)**

1. Подмена доверенного объекта в сети по-другому называется:

*Вариант 1 фишинг*

*Вариант 2 скриминг*

*Вариант 3 снифинг*

*Вариант 4 спуфинг*

2. Как называется экранирование, основанное на том, что высокочастотное электромагнитное поле ослабляется им же созданными вихревыми токами обратного напряжения?

*Вариант 1 магнитостатическое*

*Вариант 2 электромагнитное*

*Вариант 3 электростатическое*

3 Какой компонент комплекса для перехвата радиосигналов предназначен для определения параметров сигнала (частота, вид модуляции, структура кода и т.п.)?

*Вариант 1 антенна*

*Вариант 2 радиоприемник*

*Вариант 3 регистрирующее устройство*

*Вариант 4 анализатор технических характеристик сигнала*

*Вариант 5 радиопеленгатор*

4. Злоумышленник украл реквизиты банковской карты Анны и снял с ее счета деньги. Какой ущерб нанес злоумышленник Анне?

*Вариант 1 опосредованный*

*Вариант 2 непосредственный*

*Вариант 3 явный*

*Вариант 4 сильный*

5. Какой орган исполнительной власти осуществляет контроль в области криптографической защиты информации?

*Вариант 1 ФСБ России*

*Вариант 2 МВД России*

*Вариант 3 ФСТЭК России*

*Вариант 4 Роскомнадзор*

6. Задание:

Как называется DOS-атака, которая использует ping-пакеты в широковещательном режиме?

*Вариант 1 TCP flood*

*Вариант 2 Smurf*

*Вариант 3 ICMP flood*

*Вариант 4 UDP flood*

7. Какой документ содержит в себе стратегические национальные приоритеты, цели и меры в области внутренней и внешней политики России, определяющие состояние национальной безопасности и уровень устойчивого развития государства на долгосрочную перспективу?

*Вариант 1 Стратегия национальной безопасности Российской Федерации*

*Вариант 2 Федеральный закон «О государственной тайне»*

*Вариант 3 Федеральный закон «Об информации, информационных технологиях и о защите информации»*

*Вариант 4 Доктрина информационной безопасности Российской Федерации*

8. Какие приборы можно использовать для выявления пустот в ограждающих конструкциях?

*Вариант 1 интерсепторы*

*Вариант 2 рентгеновские установки*

*Вариант 3 тепловизоры*

*Вариант 4 сканирующие приемники*

9. Ослабление звука в параболическом микрофоне тем сильнее, чем:

*Вариант 1 меньше угол волны по отношению к оси*

*Вариант 2 чем больше диаметр микрофона*

*Вариант 3 чем меньше диаметр микрофона*

*Вариант 4 больше угол волны по отношению к оси*

10. Как называется излучение, которое позволяет построить изображение внутреннего строения радиозакладки?

*Вариант 1 кинетическое*

*Вариант 2 потенциальное*

*Вариант 3 тепловое*

*Вариант 4 тормозное*

11. Какую скорость сканирования каналов имеет сканирующий приемник Winradio 1000?

*Вариант 1 50 каналов/с*

*Вариант 2 30 каналов/с*

*Вариант 3 10 каналов/c*

*Вариант 4 100 каналов/с*

12. К какому типу угроз в соответствии с Доктриной информационной безопасности можно отнести несанкционированный доступ к персональной информации?

*Вариант 1 угрозы информационному обеспечению государственной политики России*

*Вариант 2 угрозы конституционным правам и свободам человека и гражданина, индивидуальному, групповому*

*и общественному сознаниям, духовному возрождению России*

*Вариант 3 угрозы безопасности информационных и телекоммуникационных средств и систем*

*Вариант 4 угрозы развитию российской индустрии информации*

13. Как называется подтверждение соответствия объектов требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров?

*Вариант 1 сертификация*

*Вариант 2 аккредитация*

*Вариант 3 лицензирование*

*Вариант 4 аттестация*

14. Как называется процесс, целью которого является выявление возможно внедренных специальных электронных средств перехвата информации, содержащей государственную тайну, в ограждающих конструкциях, предметах мебели и интерьера выделенных помещений?

*Вариант 1 специальное исследование*

*Вариант 2 специальный контроль*

*Вариант 3 специальная проверка*

*Вариант 4 специальное обследование*

15. Что необходимо получить для официального подтверждения эффективности используемых мер и средств по защите информации на объекте информатизации?

*Вариант 1 аттестат*

*Вариант 2 сертификат*

*Вариант 3 лицензию*

*Вариант 4 решение*

16. К основным показателям ТКУИ относятся: (Ответ считается верным, если отмечены все правильные варианты ответов.)

*Вариант 1 мощность*

*Вариант 2 ширина спектра*

*Вариант 3 длина канала*

*Вариант 4 относительная информативность*

*Вариант 5 пропускная способность*

17. Какие уязвимости присущи протоколу UDP?

*Вариант 1 отсутствие механизма предотвращения перегрузок буфера*

*Вариант 2 отсутствие аутентификации сообщений об изменении параметров маршрута*

*Вариант 3 аутентификация на базе открытого текста*

*Вариант 4 отсутствие поддержки аутентификации заголовков сообщений*

18. Информация о состоянии окружающей среды относится к :(Отметьте один правильный вариант ответа.)

*Вариант 1 государственной тайне*

*Вариант 2 конфиденциальной информации*

*Вариант 3 информации ограниченного доступа*

*Вариант 4 общедоступной информации*

19. Как называется совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов, в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров?

*Вариант 1 локальная вычислительная сеть*

*Вариант 2 объект информатизации*

*Вариант 3 объект защиты*

*Вариант 4 автоматизированная система*

20. Как называется модель нарушителя, которая отражает систему принятых руководством объекта защиты взглядов на контингент потенциальных нарушителей, причины и мотивацию их действий, преследуемые цели и общий характер действий в процессе подготовки и совершения акций воздействия?

*Вариант 1 косвенная*

*Вариант 2 количественная*

*Вариант 3 содержательная*

*Вариант 4 математическая*

21. Установка антивирусного обеспечения относится к:

*Вариант 1 организационным мерам обеспечения безопасности*

*Вариант 2 техническим мерам обеспечения безопасности*

*Вариант 3 физическим мерам обеспечения безопасности*

*Вариант 4 морально-этическим мерам обеспечения безопасности*

22. Какой участник системы аттестации ведет информационную базу аттестованных им объектов информатизации?

*Вариант 1 испытательная лаборатория*

*Вариант 2 орган по аттестации*

*Вариант 3 ФСТЭК*

*Вариант 4 заявитель*

23. Задание:

На какие два класса делятся угрозы по степени мотивации?

*Вариант 1 естественные и искусственные*

*Вариант 2 выгодные и невыгодные*

*Вариант 3 пассивные и активные*

*Вариант 4 непреднамеренные и преднамеренные*

24. Целью какой атаки является нарушение доступности информации для законных субъектов информационного обмена?

*Вариант 1 анализ сетевого трафика*

*Вариант 2 внедрение ложного объекта*

*Вариант 3 отказ в обслуживании*

*Вариант 4 сканирование сети*

25. Какое напряжение обычно используется для питания маленьких проводных микрофонов?

*Вариант 1 220 В*

*Вариант 2 30-45 В*

*Вариант 3 100-150В*

*Вариант 4 9-15 В*

26. Как называется юридическое лицо или индивидуальный предприниматель, обратившиеся в лицензирующий орган с заявлением о предоставлении лицензии на осуществление конкретного вида деятельности?

*Вариант 1 правообладатель*

*Вариант 2 лицензиат*

*Вариант 3 регулятор*

*Вариант 4 соискатель лицензии*

27. В соответствии с каким документом классифицируются АС, обрабатывающие конфиденциальную информацию?

*Вариант 1 ФЗ «Автоматизированные системы»*

*Вариант 2 РД Гостехкомиссии России «Защита информации. Специальные защитные знаки. Классификация и общие требования»*

*Вариант 3 ФЗ «Об информации, информационных технологиях и о защите информации»*

*Вариант 4 РД Гостехкомиссии России «Автоматизированные системы. Защита от НСД к информации.»*

28. Как называется состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право?

*Вариант 1 целостность*

*Вариант 2 доступность*

*Вариант 3 неотказуемость*

*Вариант 4 конфиденциальность*

29. Что выполняет фильтрацию сетевого трафика?

*Вариант 1 антивирус*

*Вариант 2 система обнаружения вторжений*

*Вариант 3 межсетевой экран*

*Вариант 4 браузер*

30. Какой орган государственной власти осуществляет контроль за соблюдением лицензиатом лицензионных требований и условий в области технической защиты конфиденциальной информации некриптографическими методами?

*Вариант 1 МВД России*

*Вариант 2 ФСБ России*

*Вариант 3 ФСТЭК России*

*Вариант 4 Роскомнадзор*

**Примеры типовых тестовых заданий (7 семестр)**

1. Задание:

При разработке алгоритма НМАС преследовались следующие цели: (Ответ считается верным, если отмечены все правильные варианты ответов.)

*Вариант 1 существенно увеличить скорость работы алгоритма по сравнению со скоростью работы соответствующей хэш-функцией*

*Вариант 2 возможность использования секретных ключей и простота работы с ними*

*Вариант 3 сохранение скорости работы алгоритма, близкой к скорости работы соответствующей хэш-функции*

2. Задание:

При использовании криптографии на эллиптических кривых в качестве аналога алгоритма Диффи-Хеллмана в уравнении PA = nA×G точка PA называется

*Вариант 1 нулевым элементом*

*Вариант 2 генерирующей точкой*

*Вариант 3 открытым ключом*

3. Задание:

Конфиденциальность – это

(Отметьте один правильный вариант ответа.)

*Вариант 1 невозможность несанкционированного изменения данных*

*Вариант 2 невозможность несанкционированного доступа к данным*

*Вариант 3 невозможность несанкционированного просмотра данных*

4. Задание:

Выберите правильное утверждение

(Отметьте один правильный вариант ответа.)

*Вариант 1 в основе алгоритма Rijndael лежит сеть Фейштеля смешанного типа с 4 ветвями*

*Вариант 2 в основе алгоритма Rijndael не лежит сеть Фейштеля*

*Вариант 3 в основе алгоритма Rijndael лежит традиционная сеть Фейштеля*

5. Задание:

В алгоритме RC6 используются следующие операции

(Ответ считается верным, если отмечены все правильные варианты ответов.)

*Вариант 1 циклический сдвиг на несколько битов*

*Вариант 2 XOR слов*

*Вариант 3 S-box*

6. Задание:

В алгоритмах симметричного шифрования секретным должен быть:

(Отметьте один правильный вариант ответа.)

*Вариант 1 весь алгоритм симметричного шифрования*

*Вариант 2 ключ*

*Вариант 3 отдельные элементы алгоритма симметричного шифрования (такие как S-box)*

7. Задание:

Выберите правильное утверждение

(Ответ считается верным, если отмечены все правильные варианты ответов.)

*Вариант 1 подпись должна быть битовым образцом, который зависит от подписываемого сообщения*

*Вариант 2 подпись должна обеспечивать невозможность просмотра сообщения*

*Вариант 3 подпись должна использовать некоторую уникальную информацию отправителя для предотвращения подделки или отказа*

8. Задание:

Выберите правильное утверждение:

(Ответ считается верным, если отмечены все правильные варианты ответов.)

*Вариант 1 в основе алгоритма DES лежит сеть Фейштеля*

*Вариант 2 в алгоритме DES используются S-boxes*

*Вариант 3 в алгоритме DES используется умножение по модулю 216 + 1.*

9. Задание:

Длина хэш-кода хэш-функции ГОСТ 3411 равна

(Отметьте один правильный вариант ответа.)

*Вариант 1 128 бит*

*Вариант 2 160 бит*

*Вариант 3 256 бит*

10. Задание:

Укажите, какая подпись является детерминированной

(Отметьте один правильный вариант ответа.)

*Вариант 1 DSS*

*Вариант 2 ГОСТ 3410*

*Вариант 3 RSA*

11. Задание:

Функция Эйлера – это

(Отметьте один правильный вариант ответа.)

*Вариант 1 aΦ (n) ≡ 1 mod n для всех взаимнопростых a и n, где Φ(n) - число положительных чисел, меньших n и взаимнопростых с n*

*Вариант 2 число положительных чисел, меньших n и взаимнопростых с n*

*Вариант 3 an-1 ≡ 1 mod n, если n - простое*

12. Задание:

S-box’ом называется

(Отметьте один правильный вариант ответа.)

*Вариант 1 переупорядочивание битов в блоке*

*Вариант 2 табличная подстановка, при которой группа битов отображается в другую группу битов*

*Вариант 3 циклический сдвиг на переменное число битов*

13. Задание:

Какому полиному соответствует шестнадцатеричное число F8

(Отметьте один правильный вариант ответа.)

*Вариант 1 x7 + x6 + x5 + x4 + x3 + x2 + x + 1*

*Вариант 2 x7 + x6 + x5 + x4 + x3*

*Вариант 3 x6 + x5 + x4 + 1*

14. Задание:

Длина блоков, на которые делится сообщение, в хэш-функции MD5 равна

(Отметьте один правильный вариант ответа.)

*Вариант 1 128 бит*

*Вариант 2 512 бит*

*Вариант 3 1024 бит*

15. Задание:

Выберите правильное утверждение:

(Отметьте один правильный вариант ответа.)

*Вариант 1 в криптографии с использованием эллиптических кривых все значения вычисляются по модулю n, где n – произведение двух простых чисел*

*Вариант 2 в криптографии с использованием эллиптических кривых все значения вычисляются по модулю произвольного числа р*

*Вариант 3 в криптографии с использованием эллиптических кривых все значения вычисляются по модулю простого числа р*

16. Задание:

Алгоритм НМАС позволяет

(Ответ считается верным, если отмечены все правильные варианты ответов.)

*Вариант 1 использовать без модификаций уже имеющиеся хэш-функции*

*Вариант 2 выполнять сжатие сообщения*

*Вариант 3 осуществлять замену встроенной хэш-функции на более быстрые или более стойкие*

17. Задание:

Последовательность случайных чисел должна быть

(Отметьте один правильный вариант ответа.)

*Вариант 1 иметь равномерное распределение*

*Вариант 2 монотонно возрастающей*

*Вариант 3 монотонно убывающей*

18. Задание:

Для передачи коротких сообщений лучше всего соответствуют режимы

(Отметьте один правильный вариант ответа.)

*Вариант 1 CBC*

*Вариант 2 ECB*

*Вариант 3 OFB*

*Вариант 4 CFB*

19. Задание:

Шифрование и дешифрование имеют аналогичные функции в алгоритмах

(Ответ считается верным, если отмечены все правильные варианты ответов.)

*Вариант 1 Twofish*

*Вариант 2 MARS*

*Вариант 3 Serpent*

*Вариант 4 RC6*

*Вариант 5 Rijndael*

20. Задание:

Хэш-функции предназначены для

(Отметьте один правильный вариант ответа.)

*Вариант 1 получения «отпечатков пальцев» сообщения*

*Вариант 2 шифрования сообщения*

*Вариант 3 сжатия сообщения*

21. Задание:

Алгоритм RSA может использоваться для

(Ответ считается верным, если отмечены все правильные варианты ответов.)

*Вариант 1 шифрования*

*Вариант 2 подписывания*

*Вариант 3 обмена общим секретом*

22. Задание:

Алгоритм Twofish обладает следующим свойством

(Отметьте один правильный вариант ответа.)

*Вариант 1 имеет самое быстрое шифрование/дешифрование*

*Вариант 2 имеет самое быстрое установление ключа*

*Вариант 3 имеет возможность вычисления подключей на лету*

23. Задание:

Программное выполнение алгоритмов не очень сильно изменяется в зависимости от длины

ключа

(Ответ считается верным, если отмечены все правильные варианты ответов.)

*Вариант 1 Rijndael*

*Вариант 2 MARS*

*Вариант 3 Serpent*

*Вариант 4 Twofish*

*Вариант 5 RC6*

24. Задание:

Шифрование/дешифрование с использованием эллиптических кривых выполняется

следующим образом:

(Отметьте один правильный вариант ответа.)

*Вариант 1 участник А выбирает случайное целое положительное число k и вычисляет зашифрованное сообщение Cm, являющееся точкой на эллиптической кривой Cm = {k ×G }*

*Вариант 2 участник А выбирает случайное целое положительное число k и вычисляет зашифрованное сообщение Cm, являющееся точкой на эллиптической кривой Cm = { Pm + k ×PB}*

*Вариант 3 участник А выбирает случайное целое положительное число k и вычисляет зашифрованное сообщение Cm, являющееся точкой на эллиптической кривой Cm = {k ×G, Pm + k ×PB}*

25. Задание:

Выберите правильное высказывание

(Отметьте один правильный вариант ответа.)

*Вариант 1 криптография с использованием эллиптических кривых может использоваться для шифрования сообщения*

*Вариант 2 криптография с использованием эллиптических кривых не может использоваться для шифрования сообщения*

26. Задание:

Для увеличения стойкости алгоритма количество раундов следует

(Отметьте один правильный вариант ответа.)

*Вариант 1 удвоить*

*Вариант 2 уменьшить*

*Вариант 3 увеличить*

27. Задание:

Выберите правильное высказывание

(Отметьте один правильный вариант ответа.)

*Вариант 1 алгоритм Blowfish использует постоянные S-boxes*

*Вариант 2 алгоритм Blowfish не использует S-boxes*

*Вариант 3 алгоритм Blowfish использует переменные S-boxes, зависящие от ключа*

28. Задание:

Самое быстрое установление ключа

(Отметьте один правильный вариант ответа.)

*Вариант 1 Rijndael*

*Вариант 2 RC6*

*Вариант 3 Serpent*

*Вариант 4 MARS*

*Вариант 5 Twofish*

29. Задание:

Выберите правильное высказывание

(Отметьте один правильный вариант ответа.)

*Вариант 1 в алгоритме Rijndael забеливание выполняется с использованием ключа*

*Вариант 2 в алгоритме Rijndael отсутствует забеливание*

*Вариант 3 в алгоритме Rijndael забеливание выполняется без использования ключа*

30. Задание:

Выберите правильное утверждение:

(Отметьте один правильный вариант ответа.)

*Вариант 1 ключ сессии должен быть более защищенным, чем мастер-ключ*

*Вариант 2 мастер-ключ должен быть более защищенным, чем ключ сессии*

*Вариант 3 мастер-ключ и ключ сессии должны иметь одинаковую степень защиты*

**Вопросы для подготовки к дифференцированному зачету (7 семестр)**

1. Понятие информационной безопасности. Вопросы информационной безопасности в системе обеспечения национальной безопасности.
2. Основные составляющие и аспекты информационной безопасности.
3. Классификация угроз информационной безопасности: для личности, для общества, для государства.
4. Понятие информационной войны. Особенности информационной войны. Понятие информационного превосходства.
5. Концепция «информационной войны» по оценкам российских спецслужб.
6. Понятие информационного оружия. Что отличает информационное оружие от обычных средств поражения?
7. Сфера применения информационного оружия.
8. Особенности информационного оружия. Организация защиты.
9. Основные задачи в сфере обеспечения информационной безопасности.
10. Отечественные стандарты в области информационной безопасности
11. Зарубежные стандарты в области информационной безопасности
12. Понятие защиты информации. Какая система считается безопасной? Какая система считается надёжной?
13. Основные критерии оценки надежности: политика безопасности и гарантированность.
14. Понятие государственной тайны. Понятие профессиональной тайны.
15. Понятие коммерческой тайны. Понятие служебной тайны. Понятие банковской тайны.
16. Основные конституционные гарантии по охране и защите прав и свобод в информационной сфере.
17. Понятие надежности информации в автоматизированных системах обработки данных. Что понимается под системной защитой информации.
18. Уязвимость информации в автоматизированных системах обработки данных.
19. Элементы и объекты защиты в автоматизированных системах обработки данных.
20. Методы защиты информации от преднамеренного доступа.
21. Защита информации от исследования и копирования.
22. Опознавание с использованием простого пароля. Метод обратимого шифрования.
23. Использование динамически изменяющегося пароля. Методы модификации схемы простых паролей.
24. Использование динамически изменяющегося пароля. Метод «запрос-ответ»
25. Использование динамически изменяющегося пароля. Функциональные методы
26. Криптографические методы защиты информации в автоматизированных системах. Основные направления использования криптографических методов. Симметричные криптосистемы. Системы с открытым ключом.
27. Электронная (цифровая) подпись. Цели применения электронной подписи.
28. Понятие криптостойкости шифра. Требования к криптографическим системам защиты информации.
29. Классификация методов криптографического закрытия.
30. Особенности защиты информации в персональных ЭВМ. Основные цели защиты информации.
31. Угрозы информации в персональных ЭВМ.
32. Обеспечение целостности информации в ПК. Физическая зашита ПК и носителей информации.
33. Защита ПК от несанкционированного доступа.
34. Способы опознавания (аутентификации) пользователей и используемых компонентов обработки информации. Дать краткую характеристику.
35. Классификация закладок. Причины защиты ПК от закладок. Аппаратные закладки.
36. Программные закладки. Классификация критериев вредоносного воздействия закладок.
37. Общие характеристики закладок.
38. Методы и средства защиты от закладок.
39. Компьютерный вирус. Какая программа считается зараженной.
40. По каким признакам классифицируются вирусы?
41. Способы заражения программ. Стандартные методы заражения.
42. Как работает вирус?
43. Методы защиты от вирусов.
44. Антивирусные программы. Программы-детекторы. Программы-доктора.
45. Антивирусы-полифаги. Эвристические анализаторы.
46. Программы-ревизоры. Программы-фильтры.
47. Цели, функции и задачи защиты информации в сетях ЭВМ. Угрозы безопасности для сетей передачи данных.
48. В чём заключаются задачи защиты в сетях передачи данных?
49. Проблемы защиты информации в вычислительных сетях.
50. Понятие сервисов безопасности: идентификация / аутентификация, разграничение доступа.
51. Понятие сервисов безопасности: шифрование, контроль целостности, контроль защищённости, обнаружение отказов и оперативное восстановление.
52. Архитектура механизмов защиты информации в сетях ЭВМ.

**Типовые практические задания**

1. Разработать политику безопасности организации по предоставленным данным
2. Защита информации в компьютерной системе от случайных угроз
3. Создание и управление учетными записями пользователей
4. Обеспечение безопасности ресурсов с помощью разрешений файловой системы ntfs
5. Аудит ресурсов и событий системы защиты
6. Настройка параметров безопасности подключения к интернет
7. Настройка системных параметров безопасности
8. Повышение безопасности информации встроенными средствами шифрования операционной системы
9. Установка и настройка agnitum outpost firewall
10. Установка и настройка антивирусных программ
11. Программная реализация шифра Цезаря
12. Программная реализация шифра Виженера
13. Программная реализация шифра RSA
14. Программная реализация шифра ГОСТ 28147.89
15. Программная реализация алгоритма хеширования MD5
16. Программная реализация алгоритма ЭЦП

**4. Критерии оценки**

**4.1. Практическая работа:**

«5» – все задания выполнены

«4» – наблюдались неточности при выполнении работы

«3» – наблюдались ошибки при выполнении работы

«2» – работа выполнена менее 50 %

**4.2. Тестовые задания:**

|  |  |  |
| --- | --- | --- |
| Процент результативности (правильных ответов) | Качественная оценка индивидуальных образовательных достижений | |
| балл (отметка) | вербальный аналог |
| 86 ÷ 100 | 5 | отлично |
| 70 ÷ 85 | 4 | хорошо |
| 55 ÷ 69 | 3 | удовлетворительно |
| менее 55 | 2 | не удовлетворительно |

**4.3 Теоретические вопросы**

|  |  |
| --- | --- |
| Оценка | Критерии |
| *«отлично»* | Дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний по дисциплине, доказательно раскрыты основные положения вопросов; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знания по предмету демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей. Ответ изложен литературным языком с использованием современной технической терминологии. Могут быть допущены недочеты в определении понятий, исправленные студентом самостоятельно в процессе ответа. |
| *«хорошо»* | Дан полный, развернутый ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, изложен литературным языком с использованием современной технической терминологии. Могут быть допущены некоторые неточности или незначительные ошибки, исправленные студентом с помощью преподавателя. |
| *«удовлетвори-тельно*» | Дан недостаточно полный и недостаточно развернутый ответ. Логика и последовательность изложения имеют нарушения. Допущены ошибки в раскрытии понятий, употреблении терминов. Студент не способен самостоятельно выделить существенные и несущественные признаки и причинно-следственные связи. В ответе отсутствуют выводы. Умение раскрыть значение обобщенных знаний не показано. Речевое оформление требует поправок, коррекции. |
| *«неудовлетворительно»* | 1) Ответ представляет собой разрозненные знания с существенными ошибками по вопросу. Присутствуют фрагментарность, нелогичность изложения. Студент не осознает связь обсуждаемого вопроса по билету с другими объектами дисциплины. Отсутствуют выводы, конкретизация и доказательность изложения. Речь неграмотная, техническая терминология не используется. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента.  2) Ответ на вопрос полностью отсутствует.  3) Отказ от ответа. |

# 5. Информационное обеспечение обучения

**Основные источники:**

1. Защита информации в компьютерных системах и сетях. Уч. пособие для технических вузов, 5-7695-1796-4, ИЦ ДМК, 2013.., 592 стр. Шаньгин В. Ф.

**Дополнительные источники:**

1. Зеркина Е. В. Информационная безопасность в системе открытого образования (для специальности 050202 – «Информатика») : учеб. – метод. пособие / Е. В. Зеркина.

– Магнитогорск : МаГУ, 2013. – 100 с.

1. Кононов, А. А. Информационное общество: общество тотального риска или общество управляемой безопасности? / А. А. Кононов. – М. : Едиториал УРСС, 2013. – с. 6 -20.
2. Уорли Б. Интернет : реальные и мнимые угрозы / пер. с англ. – М. : КУДИЦОБРАЗ, 2013. -320 с.
3. Джонсон С. как защитить детей от опасностей Интернета : вирусов, программ-шпионов, спама, порносайтов, всплывающих окон / Саймон Джонсон ; пер. с англ. Е. А. Ивановой. – М. : НТ Пресс, 2013. – 304 с. : ил.

Андреева Н. В., Асеев Х. М. Обеспечение комплексной безопасности в образовательном учреждении. Безопасность в образовательном учреждении: настольная книга руководителя / Н. В. Андреева, Х. М. Асеев и др. – М. : Айрис-Пресс, 2013. – 247 с.

1. ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.
2. ГОСТ 28147-89. Государственный стандарт Российской Федерации. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
3. ГОСТ Р 34.10-94. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной подписи на базе асимметричного криптографического алгоритма.
4. ГОСТ Р 34.11-94. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хеширования.
5. ГОСТ Р 34.10-2001 Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи

**ИНТЕРНЕТ-РЕСУРСЫ**

1. <http://www.intuit.ru>
2. <http://habrahabr.ru/blogs/programming/>
3. <http://phpclub.ru/>
4. <http://www.webscript.ru/>