Федеральное агентство морского и речного транспорта
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Государственный университет морского и речного флота имени адмирала С.О. Макарова»

Котласский филиал ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова»

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«ОП.13 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

ПРОГРАММЫ ПОДГОТОВКИ СПЕЦИАЛИСТОВ СРЕДНЕГО ЗВЕНА
по специальности
09.02.07 Информационные системы и программирование

квалификация
специалист по информационным системам

Котлас
2023

СОГЛАСОВАНА
Заместитель директора по учебно-методической работе филиала

_____Н.Е. Гладышева

19 05 2023

УТВЕРЖДЕНА
Директор филиала

_____ **О.В. Шергина**

_____ **2023**

ОДОБРЕНА
на заседании цикловой комиссии
информационных технологий
Протокол от 19.04.2023 № 8

Председатель _____ Д.В. Жигалов

РАЗРАБОТЧИК:
Кубраков Сергей Петрович– преподаватель КРУ Котласского филиала ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова»

Рабочая программа учебной дисциплины «ОП.13. Основы информационной безопасности» разработана в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования, утвержденным Министерства образования и науки Российской Федерации от 9 декабря 2016 г. № 1547 (зарегистрирован Министерством юстиции Российской Федерации 26 декабря 2016 г., регистрационный № № 44936) по специальности 09.02.07 «Информационные системы и программирование» с изменениями и дополнениями от 17 декабря 2020 г. №747, профессиональным стандартом 06.015 «Специалист по информационным системам», утвержденным приказом Министерства труда и социальной защиты Российской Федерации от 18 ноября 2014 г. № 896н (зарегистрирован Министерством юстиции Российской Федерации 24 декабря 2014 г., регистрационный № 35361), примерной основной образовательной программой № П-24 государственного реестра ПООП, со стандартами Ворлдскиллс Россия, с учётом Стратегии развития воспитания в Российской Федерации на период до 2025 года, рабочей программы воспитания.

СОДЕРЖАНИЕ

1.ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ

УЧЕБНОЙ ДИСЦИПЛИНЫ «ОП.13 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

1.1. Место дисциплины в структуре основной образовательной программы:

Учебная дисциплина «ОП.13. Основы информационной безопасности» является обязательной частью общеобразовательного цикла ОП.00 программы подготовки специалистов среднего звена в соответствии с ФГОС СПО

по специальности: 09.02.07 Информационные системы и программирование

укрупнённой группы специальностей: 09.00.00 Информатика и вычислительная техника.

Особое значение дисциплина имеет при формировании и развитии общих компетенций (ОК 01, ОК 02, ОК 05, ОК 09), профессиональных компетенций (ПК 5.3, ПК 6.5, ПК 7.3, ПК 7.5) в соответствии с ФГОС СПО, личностных результатов реализации программы воспитания (ЛР 4, ЛР 10, ЛР 13, ЛР 14, ЛР 15, ЛР 16).

1.2. Цель и планируемые результаты освоения дисциплины:

В рамках программы учебной дисциплины обучающимися осваиваются умения и знания в соответствии с ФГОС и ПООП

Код ОК, ПК	Умения	Знания
ОК 01, ОК 02, ОК 05, ОК 09, ПК 5.3, ПК 6.5, ПК 7.3, ПК 7.5	- осуществлять техническое сопровождение, сохранение и восстановление базы данных информационной системы; - составлять планы резервного копирования; - определять интервал резервного копирования; - формировать требования к конфигурации локальных компьютерных сетей и серверного оборудования, необходимые для работы баз данных и серверов в рамках поставленной задачи; - разрабатывать политику безопасности SQL сервера, базы данных и отдельных объектов базы данных	- национальной и международной системы стандартизации и сертификации и систему обеспечения качества продукции; - терминология и методы резервного копирования, восстановление информации в информационной системе; - требования к безопасности сервера базы данных

Освоение содержания учебной дисциплины обеспечивает достижение обучающимися следующих личностных результатов программы воспитания:

Личностные результаты реализации программы воспитания	
Код	**Формулировка**
ЛР 4	Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа»
ЛР 10	Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой

Личностные результаты реализации программы воспитания, определённые отраслевыми требованиями к деловым качествам личности	
ЛР 13	Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации
ЛР 14	Демонстрирующий навыки анализа и интерпретации информации из различных источников с учетом нормативно-правовых норм
ЛР 15	Демонстрирующий готовность и способность к образованию, в том числе самообразованию, на протяжении всей жизни; сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности
Личностные результаты реализации программы воспитания, определённые субъектом Российской Федерации	
ЛР 16	Обладающий профессиональными качествами, необходимыми для дальнейшего развития производственных отраслей и сферы услуг во всех регионах Российской Федерации

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем часов**
Объем образовательной программы учебной дисциплины	**88**
в т. ч. в форме практической подготовки	18
в т. ч.:	
теоретические занятия	52
практические занятия	18
Самостоятельная работа обучающегося	8
Консультации	4
Промежуточная аттестация в форме экзамена	6

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Коды компетенций и личностных результатов, формированию которых способствует элемент программы
1	2	3	4
Введение	**Содержание учебного материала**	**2**	**ОК 01, ЛР 4, ЛР 10, ЛР 13, ЛР 14, ЛР 15, ЛР 16**
	1. Введение. История информационной безопасности. Актуальность информационной безопасности.	2	
Раздел 1. Угрозы информационной безопасности		**4**	**ОК 01, ОК 02, ОК 05, ОК 09, ПК 5.3, ПК 6.5, ПК 7.3, ПК 7.5, ЛР 4, ЛР 10, ЛР 13, ЛР 14, ЛР 15, ЛР 16**
Тема 1.1. Основные угрозы и принципы информационной безопасности	**Содержание учебного материала**	**4**	
	1. Основные принципы информационной безопасности: целостность, доступность, конфиденциальность.	2	ОК 01, ОК 02, ОК 05, ОК 09, ПК 5.3, ПК 6.5, ПК 7.3, ПК 7.5, ЛР 4, ЛР 10, ЛР 13, ЛР 14, ЛР 15,
	2. Понятие уязвимости, угрозы, источника угрозы информационной безопасности, их классификации.	2	

			ЛР 16
Раздел 2. Нормативно-правовые основы информационной безопасности		**6**	**ОК 01, ОК 02, ОК 05, ОК 09, ПК 5.3, ПК 6.5, ПК 7.3, ПК 7.5, ЛР 4, ЛР 10, ЛР 13, ЛР 14, ЛР 15, ЛР 16**
Тема 2.1. Правовое обеспечение информационной безопасности	**Содержание учебного материала**	**2**	ОК 01, ОК 02, ОК 05, ОК 09, ПК 5.3, ПК 6.5, ПК 7.3, ПК 7.5, ЛР 4, ЛР 10, ЛР 13, ЛР 14, ЛР 15, ЛР 16
	1. Российское законодательство в области информационной безопасности. Ответственность за нарушение законодательства в информационной сфере.	2	
Тема 2.2. Стандарты информационной безопасности	**Содержание учебного материала**	**4**	ОК 01, ОК 02, ОК 05, ОК 09, ПК 5.3, ПК 6.5, ПК 7.3, ПК 7.5, ЛР 4, ЛР 10, ЛР 13, ЛР 14, ЛР 15, ЛР 16
	1. Международные стандарты информационной безопасности. «Оранжевая книга». ISO/IEC 15408 «Общие критерии оценки безопасности информационных технологий». Отечественные стандарты информационной безопасности.	4	
Раздел 3. Организационно-технические и режимные методы обеспечения информационной безопасности		**10**	**ОК 01, ОК 02, ОК 05, ОК 09, ПК 5.3,**

			ПК 6.5, ПК 7.3, ПК 7.5, ЛР 4, ЛР 10, ЛР 13, ЛР 14, ЛР 15, ЛР 16
Тема 3.1. Административный уровень информационной безопасности	**Содержание учебного материала**	**4**	ОК 01, ОК 02, ОК 05, ОК 09, ПК 5.3, ПК 6.5, ПК 7.3, ПК 7.5, ЛР 4, ЛР 10, ЛР 13, ЛР 14, ЛР 15, ЛР 16
	1. Понятие политики информационной безопасности организации. Эффективные и неэффективные политики.	2	
	В том числе практических занятий	**2**	
	Практическое занятие №1. Анализ политики информационной безопасности.	2	
Тема 3.2. Процедурный уровень информационной безопасности	**Содержание учебного материала**	**6**	ОК 01, ОК 02, ОК 05, ОК 09, ПК 5.3, ПК 6.5, ПК 7.3, ПК 7.5, ЛР 4, ЛР 10, ЛР 13, ЛР 14, ЛР 15, ЛР 16
	1. Управление персоналом. Физическая защита объектов информатизации. Поддержание работоспособности. Реагирование на нарушение режима безопасности. Планирование восстановительных работ.	4	
	В том числе практических занятий	**2**	
	Практическое занятие №2. Организация физической защиты и поддержания работоспособности.	2	
Раздел 4. Программно-технические средства обеспечения информационной безопасности		**36**	**ОК 01, ОК 02, ОК 05, ОК 09, ПК 5.3, ПК 6.5, ПК 7.3, ПК 7.5, ЛР 4, ЛР 10, ЛР 13, ЛР 14, ЛР 15, ЛР 16**
Тема 4.1. Средства управления	**Содержание учебного материала**	**10**	ОК 01, ОК 02, ОК 05, ОК 09, ПК 5.3,
	1. Принципы управления доступом. Дискреционное управление доступом. Мандатное и ролевое управление доступом. Идентификация и аутентификация.	8	

доступом	Журналирование и аудит.		ПК 6.5, ПК 7.3, ПК 7.5, ЛР 4, ЛР 10, ЛР 13, ЛР 14, ЛР 15, ЛР 16
	В том числе практических занятий	**2**	
	Практическое занятие №3. Изучение средств управления доступом.	2	
Тема 4.2. Криптографические средства защиты информации	**Содержание учебного материала**	**12**	ОК 01, ОК 02, ОК 05, ОК 09, ПК 5.3, ПК 6.5, ПК 7.3, ПК 7.5, ЛР 4, ЛР 10, ЛР 13, ЛР 14, ЛР 15, ЛР 16
	1. Криптология. Криптография. Криптоанализ. Классификация методов шифрования. Этапы развития криптографии.	2	
	2. Симметричные криптосистемы. Асимметричные криптосистемы. ЭЦП. Алгоритмы шифрования. Реализация алгоритмов шифрования	6	
	В том числе практических занятий	**4**	
	Практическое занятие №4. Изучение методов симметричного шифрования. Практическое занятие №5. Изучение программных средств шифрования информации.	4	
Тема 4.3. Средства защиты от вредоносных программ	**Содержание учебного материала**	**8**	ОК 01, ОК 02, ОК 05, ОК 09, ПК 5.3, ПК 6.5, ПК 7.3, ПК 7.5, ЛР 4, ЛР 10, ЛР 13, ЛР 14, ЛР 15, ЛР 16
	1. Классификация вредоносных программ. Пути распространения. Вред, наносимый вредоносными программами. Признаки заражения вредоносными программами.	4	
	2. Методы защиты от вредоносных программ. Антивирусные программы.	2	
	В том числе практических занятий	**2**	
	Практическое занятие №6. Изучение работы антивирусной программы.	2	
Тема 4.4. Средства резервного копирования	**Содержание учебного материала**	**6**	ОК 01, ОК 02, ОК 05, ОК 09, ПК 5.3, ПК 6.5, ПК 7.3, ПК 7.5, ЛР 4, ЛР 10, ЛР 13, ЛР 14, ЛР 15, ЛР 16
	1. Системы хранения данных. RAID-массивы, сетевые хранилища, ленточные библиотеки и т.п. Резервное копирование информации. Методы и средства резервного копирования. Схемы ротации носителей резервных копий.	4	
	В том числе практических занятий	**2**	
	Практическое занятие №7. Изучение средств резервного копирования.	2	

Раздел 5. Комплексное обеспечение информационной безопасности		**20**	**ОК 01, ОК 02, ОК 05, ОК 09, ПК 5.3, ПК 6.5, ПК 7.3, ПК 7.5, ЛР 4, ЛР 10, ЛР 13, ЛР 14, ЛР 15, ЛР 16**
Тема 5.1. Защита информации в персональных компьютерах	**Содержание учебного материала**	**4**	ОК 01, ОК 02, ОК 05, ОК 09, ПК 5.3, ПК 6.5, ПК 7.3, ПК 7.5, ЛР 4, ЛР 10, ЛР 13, ЛР 14, ЛР 15, ЛР 16
	1. Защита информации в персональных компьютерах.	2	
	В том числе практических занятий	**2**	
	Практическое занятие №8. Изучение средств защиты информации в ПК.	2	
Тема 5.2. Защита информации в компьютерных сетях	**Содержание учебного материала**	**16**	ОК 01, ОК 02, ОК 05, ОК 09, ПК 5.3, ПК 6.5, ПК 7.3, ПК 7.5, ЛР 4, ЛР 10, ЛР 13, ЛР 14, ЛР 15, ЛР 16
	1. Угрозы информационной безопасности в компьютерных сетях. Защита информации в компьютерных сетях. Межсетевые экраны и прокси-серверы.	6	
	В том числе практических занятий	**2**	
	Практическое занятие №9. Изучение средств защиты информации в компьютерных сетях.	2	
	Самостоятельная работа обучающихся Исследовательская работа «Разработка комплекса мер по защите рабочего места».	8	
Консультации		**4**	
Промежуточная аттестация в форме экзамена		**6**	
Всего:		**88**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Для реализации программы учебной дисциплины должны быть предусмотрены следующие специальные помещения:

Учебная аудитория «Информационные системы. Компьютерные сети. Инструментальные средства разработки. Организация и принципы построения информационных систем», оснащённая оборудованием и техническими средствами обучения: Комплект учебной мебели (столы, стулья, доска), компьютер в сборе (системный блок (Intel Celeron 2,5 GHz, 2 Gb), монитор Samsung 740N ЖК, клавиатура, мышь) - 16 шт., мультимедийный проектор NEC (переносной) - 1 шт., экран на штативе - 1 шт., локальная компьютерная сеть, коммутатор - 1 шт.

3.2. Информационное обеспечение реализации программы

Для реализации программы в библиотечном фонде имеются электронные образовательные и информационные ресурсы, в том числе рекомендованные ФУМО, для использования в образовательном процессе. При формировании библиотечного фонда учтены издания, предусмотренные примерной основной образовательной программой по специальности 09.02.07 «Информационные системы и программирование».

3.2.1. Основные электронные издания

1. Основы информационной безопасности. Баранова Е.К., Бабаш А.В. Учебник: М.: РИОР: ИНФРА-М, 2019. — 202 с. — (Среднее профессиональное образование). https://ibooks.ru/reading.php?productid=360593

2. Техническая защита информации в объектах информационной инфраструктуры. Бубнов А.А., Пржегорлинский В.Н., Фомина К.Ю. Учебник: М. : Издательский центр «Академия», 2019. — 272 с. https://academia-moscow.ru/catalogue/4893/444513/

3.2.2. Дополнительные источники:

1. Прохорова, О.В. Информационная безопасность и защита информации: учебник. Санкт-Петербург : Лань, 2020. — 124 с. https://e.lanbook.com/book/133924

3.3. Организация образовательного процесса

3.3.1. Требования к условиям проведения учебных занятий

Учебная дисциплина с целью обеспечения доступности образования, повышения его качества при необходимости может быть реализована с применением технологий дистанционного, электронного и смешанного обучения.

Электронное обучение и дистанционные образовательные технологии используются для:

– организации самостоятельной работы обучающихся (предоставление материалов в электронной форме для самоподготовки; обеспечение подготовки к практическим и лабораторным занятиям, организация возможности самотестирования и др.);

– проведения консультаций с использованием различных средств онлайн-взаимодействия (например, вебинаров, форумов, чатов) в электронно-информационной образовательной среде Котласского филиала ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова» и с применением других платформ и сервисов для организации онлайн-обучения;

– организации текущего и промежуточного контроля обучающихся и др.

Смешанное обучение реализуется посредством:

– организации сочетания аудиторной работы с работой в электронно-информационной образовательной среде Котласского филиала ФГБОУ ВО «ГУМРФ

имени адмирала С.О. Макарова» и с применением других платформ и сервисов для организации онлайн-обучения;

– регулярного взаимодействия преподавателя с обучающимися с использованием технологий электронного и дистанционного обучения;

– организации групповой учебной деятельности обучающихся в электронно-информационной образовательной среде Котласского филиала ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова» или с применением других платформ и сервисов для организации онлайн-обучения.

Основными средствами, используемыми для реализации данных технологий, являются: системы дистанционного обучения, системы организации видеоконференций, электронно-библиотечные системы, образовательные сайты и порталы, социальные сети и месенджеры и т.д.

3.3.2. Требования к условиям консультационной помощи обучающимся

Формы проведения консультаций: групповые и индивидуальные.

3.3.3. Требования к условиям организации внеаудиторной деятельности обучающихся

Реализация учебной дисциплины обеспечивается доступом каждого обучающегося к электронно-информационной образовательной среде Котласского филиала ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова» и библиотечному фонду, укомплектованному электронными учебными изданиями.

Во время самостоятельной подготовки обучающиеся обеспечиваются доступом к сети Интернет.

Доступ к электронно-информационной образовательной среде Котласского филиала ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова» и библиотечному фонду, возможен с любого компьютера, подключённого к сети Интернет. Для доступа к указанным ресурсам на территории Котласского филиала ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова» обучающиеся могут бесплатно воспользоваться компьютерами, установленными в библиотеке или компьютерными классами (во внеучебное время).

3.4. Кадровое обеспечение образовательного процесса

Квалификация педагогических работников Котласского филиала ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова», участвующих в реализации образовательной программы, а также лиц, привлекаемых к реализации образовательной программы на других условиях, в том числе из числа руководителей и работников Котласского филиала ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова» и иных организаций, должна отвечать квалификационным требованиям, указанным в квалификационных справочниках, и в профессиональном 06.015 «Специалист по информационным системам». Педагогические работники, привлекаемые к реализации программы, должны получать дополнительное профессиональное образование по программам повышения квалификации не реже 1 раза в 3 года.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения	Критерии оценки	Методы оценки
Знать: - национальной и международной системы стандартизации и сертификации и систему обеспечения качества продукции; - терминология и методы резервного копирования, восстановление информации в информационной системе; - требования к безопасности сервера базы данных.	«Отлично» - теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко. «Хорошо» - теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками. «Удовлетворительно» - теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки. «Неудовлетворительно» - теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки.	Текущий контроль в форме экспертного наблюдения и оценки результатов достижения компетенции на учебных занятиях. Промежуточная аттестация в форме: экзамен.
Уметь: - осуществлять техническое сопровождение, сохранение и восстановление базы данных информационной системы; - составлять планы резервного копирования; - определять интервал резервного копирования; - формировать требования к конфигурации локальных компьютерных сетей и серверного оборудования, необходимые для работы баз данных и серверов в рамках поставленной задачи; - разрабатывать политику безопасности SQL сервера, базы данных и отдельных объектов базы данных.		

Федеральное агентство морского и речного транспорта
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Государственный университет морского и речного флота имени адмирала С.О. Макарова»

Котласский филиал ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова»

КОМПЛЕКТ КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

«ОП.13 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

ПРОГРАММЫ ПОДГОТОВКИ СПЕЦИАЛИСТОВ СРЕДНЕГО ЗВЕНА

по специальности

09.02.07 Информационные системы и программирование

квалификация

специалист по информационным системам

Котлас
2023

СОГЛАСОВАНА
Заместитель директора по учебно-методической работе филиала

_____Н.Е. Гладышева

19 05 2023

УТВЕРЖДЕНА
Директор филиала

_____ **О.В. Шергина**

24 05 **2023**

ОДОБРЕНА
на заседании цикловой комиссии информационных технологий
Протокол от 19.04.2023 № 8

Председатель _____ Д.В. Жигалов

СОГЛАСОВАНА
Заместитель начальника отдела контроля выполнения технологических процессов и информационных технологий Управления Федеральной налоговой службы по Архангельской области и Ненецкому автономному округу

_____ М.А. Кальненков

19 05 2023

РАЗРАБОТЧИК:

Скворцов Сергей Евгеньевич – преподаватель КРУ Котласского филиала ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова»

Комплект контрольно-оценочных средств по учебной дисциплине «ОП.13 Основы информационной безопасности» разработан в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования, утвержденным Министерства образования и науки Российской Федерации от 9 декабря 2016 г. № 1547 (зарегистрирован Министерством юстиции Российской Федерации 26 декабря 2016 г., регистрационный № № 44936) по специальности 09.02.07 «Информационные системы и программирование» с изменениями и дополнениями, профессиональным стандартом 06.015 «Специалист по информационным системам», утвержденным приказом Министерства труда и социальной защиты Российской Федерации от 18 ноября 2014 г. № 896н (зарегистрирован Министерством юстиции Российской Федерации 24 декабря 2014 г., регистрационный № 35361), рабочей программы учебной дисциплины.

СОДЕРЖАНИЕ **стр.**

1. ПАСПОРТ КОМПЛЕКТА КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ «ОП.13 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

1.1. Область применения контрольно-оценочных средств

Контрольно-оценочные средства (КОС) являются частью нормативно-методического обеспечения системы оценивания качества освоения обучающимися программы подготовки специалистов среднего звена по специальности 09.02.07 «Информационные системы и программирование» и обеспечивают повышение качества образовательного процесса.

КОС по учебной дисциплине представляет собой совокупность контролирующих материалов, предназначенных для измерения уровня достижения обучающимся установленных результатов обучения.

КОС по учебной дисциплине используется при проведении текущего контроля успеваемости и промежуточной аттестации обучающихся в виде экзамена.

1.2. Результаты освоения учебной дисциплины, подлежащие проверке

Код ОК, ПК	Умения	Знания
ОК 01, ОК 02, ОК 05, ОК 09, ПК 5.3, ПК 6.5, ПК 7.3, ПК 7.5	У1- осуществлять техническое сопровождение, сохранение и восстановление базы данных информационной системы; У2- составлять планы резервного копирования; У3- определять интервал резервного копирования; У4- формировать требования к конфигурации локальных компьютерных сетей и серверного оборудования, необходимые для работы баз данных и серверов в рамках поставленной задачи; У5- разрабатывать политику безопасности SQL сервера, базы данных и отдельных объектов базы данных	З1- национальной и международной системы стандартизации и сертификации и систему обеспечения качества продукции; З2- терминология и методы резервного копирования, восстановление информации в информационной системе; З3- требования к безопасности сервера базы данных

Освоение содержания учебной дисциплины обеспечивает достижение обучающимися следующих личностных результатов программы воспитания:

Личностные результаты реализации программы воспитания	
Код	**Формулировка**
ЛР 4	Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа»
ЛР 10	Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой

Личностные результаты реализации программы воспитания, определённые отраслевыми требованиями к деловым качествам личности	
ЛР 13	Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации
ЛР 14	Демонстрирующий навыки анализа и интерпретации информации из различных источников с учетом нормативно-правовых норм
ЛР 15	Демонстрирующий готовность и способность к образованию, в том числе самообразованию, на протяжении всей жизни; сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности
Личностные результаты реализации программы воспитания, определённые субъектом Российской Федерации	
ЛР 16	Обладающий профессиональными качествами, необходимыми для дальнейшего развития производственных отраслей и сферы услуг во всех регионах Российской Федерации

2. КОДИФИКАТОР ОЦЕНОЧНЫХ СРЕДСТВ

Функциональный признак оценочного средства (тип контрольного задания)	Метод/форма контроля
Собеседование	Устный опрос, экзамен
Практические задания	Практические занятия
Тест, тестовое задание	Тестирование, экзамен

3. СИСТЕМА ОЦЕНКИ ОБРАЗОВАТЕЛЬНЫХ ДОСТИЖЕНИЙ ОБУЧАЮЩИХСЯ ПО КАЖДОМУ ОЦЕНОЧНОМУ СРЕДСТВУ

Оценка индивидуальных образовательных достижений по результатам текущего контроля успеваемости и промежуточной аттестации производится в соответствии с универсальной шкалой (таблица).

Процент результативности (правильных ответов)	Качественная оценка индивидуальных образовательных достижений	
	балл (отметка)	вербальный аналог
90 - 100	5	отлично
80 - 89	4	хорошо
70 - 79	3	удовлетворительно
менее 70	2	неудовлетворительно

Критерии оценки ответов в ходе устного опроса

Оценивается правильность ответа обучающегося на один из приведенных вопросов. При этом выставляются следующие оценки:

«Отлично» выставляется при соблюдении следующих условий:

- полно раскрыл содержание материала в объеме, предусмотренном программой, содержанием лекции и учебником;
- изложил материал грамотным языком в определенной логической последовательности, точно используя специализированную терминологию и символику;

- показал умение иллюстрировать теоретические положения конкретными примерами, применять их в новой ситуации при выполнении практического задания;
- продемонстрировал усвоение ранее изученных сопутствующих вопросов, сформированность и устойчивость используемых при ответе умений и навыков;
- отвечал самостоятельно без наводящих вопросов преподавателя. Возможны одна-две неточности при освещении второстепенных вопросов или в выкладках, которые обучающийся легко исправил по замечанию преподавателя.

«Хорошо» - ответ удовлетворяет в основном требованиям на оценку «5», но при этом имеет один из недостатков:
- в изложении допущены небольшие пробелы, не исказившие логического и информационного содержания ответа;
- допущены один-два недочета при освещении основного содержания ответа, исправленные по замечанию преподавателя;
- допущены ошибка или более двух недочетов при освещении второстепенных вопросов или в выкладках, легко исправленные по замечанию преподавателя.

«Удовлетворительно» выставляется при соблюдении следующих условий:
- неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения программного материала, имелись затруднения или допущены ошибки в определении понятий, использовании терминологии и выкладках, исправленные после нескольких наводящих вопросов преподавателя;
- обучающийся не справился с применением теории в новой ситуации при выполнении практического задания, но выполнил задания обязательного уровня сложности по данной теме;
- при знании теоретического материала выявлена недостаточная сформированность основных умений и навыков.

«Неудовлетворительно» выставляется при соблюдении следующих условий:
- не раскрыто основное содержание учебного материала;
- обнаружено незнание или непонимание обучающимся большей или наиболее важной части учебного материала;
- допущены ошибки в определении понятий, при использовании терминологии и иных выкладках, которые не исправлены после нескольких наводящих вопросов преподавателя;
- обучающийся обнаружил полное незнание и непонимание изучаемого учебного материала или не смог ответить ни на один из поставленных вопросов по изучаемому материалу.

Критерии оценки выполненного практического задания

Оценка 5 ставится за работу, выполненную полностью без ошибок и недочётов.

Оценка 4 ставится за работу, выполненную полностью, но при наличии в ней не более одной негрубой ошибки и одного недочёта, не более трёх недочётов.

Оценка 3 ставится, если обучающийся правильно выполнил не менее 2/3 всей работы или допустил не более одной грубой ошибки и двух недочётов, не более одной грубой и одной не грубой ошибки, не более трёх негрубых ошибок, одной негрубой ошибки и трёх недочётов, при наличии четырёх-пяти недочётов.

Оценка 2 ставится, если число ошибок и недочётов превысило норму для оценки 3 или правильно выполнено менее 2/3 всей работы.

Оценка 1 ставится, если обучающийся совсем не выполнил ни одного задания.

Критерии оценки выполненного тестового задания

Результат аттестационного педагогического измерения по учебной дисциплине Основы информационной безопасности для каждого обучающегося представляет собой сумму зачтенных тестовых заданий по всему тесту. Зачтенное тестовое задание соответствует одному баллу.

Критерием освоения учебной дисциплины для обучающегося является количество правильно выполненных заданий теста не менее 70 %.

Для оценки результатов тестирования предусмотрена следующая система оценивания образовательных достижений обучающихся:

- за каждый правильный ответ ставится 1 балл;
- за неправильный ответ - 0 баллов.

Тестовые оценки можно соотнести с общепринятой пятибалльной системой. Оценивание осуществляется по следующей схеме:

Процент результативности (правильных ответов)	Качественная оценка индивидуальных образовательных достижений	
	балл (отметка)	вербальный аналог
90 - 100	5	отлично
80 - 89	4	хорошо
70 - 79	3	удовлетворительно
менее 70	2	неудовлетворительно

Критерии оценки в ходе экзамена

Ответ оценивается на «отлично», если обучающийся исчерпывающе, последовательно, грамотно и логически стройно излагает материал по вопросам билета, не затрудняется с ответом при видоизменении задания, свободно справляется с решением практических задач и способен обосновать принятые решения, не допускает ошибок.

Ответ оценивается на «хорошо», если обучающийся твердо знает программный материал, грамотно и по существу его излагает, не допускает существенных неточностей при ответах, умеет грамотно применять теоретические знания на практике, а также владеет необходимыми навыками решения практических задач.

Ответ оценивается на «удовлетворительно», если обучающийся освоил только основной материал, однако не знает отдельных деталей, допускает неточности и некорректные формулировки, нарушает последовательность в изложении материала и испытывает затруднения при выполнении практических заданий.

Ответ оценивается на «неудовлетворительно», если обучающийся не раскрыл основное содержание материала, допускает существенные ошибки, с большими затруднениями выполняет практические задания.

4. БАНК КОМПЕТЕНТНОСТНО-ОЦЕНОЧНЫХ МАТЕРИАЛОВ ДЛЯ ОЦЕНКИ УСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

4.1 Текущий контроль

4.1.1. ПРАКТИЧЕСКАЯ РАБОТА

Комплект оценочных заданий №1 по Разделу 3. Организационно-технические и режимные методы обеспечения информационной безопасности, Теме 3.1. Административный уровень информационной безопасности (Аудиторная самостоятельная работа).

Название: Анализ политики информационной безопасности.

Задание: Составить модели возможных угроз и нарушителей. Произвести анализ политики информационной безопасности.

Комплект оценочных заданий №2 по Разделу 3. Организационно-технические и режимные методы обеспечения информационной безопасности, Теме 3.2. Процедурный уровень информационной безопасности (Аудиторная самостоятельная работа).
Название: Организация физической защиты и поддержания работоспособности.
Задание: Составить перечень средств защиты серверной:
размещение, сигнализация, средства видеонаблюдения, обеспечение бесперебойного питания, средств резервного копирования.

Комплект оценочных заданий №3 по Разделу 4. Программно-технические средства обеспечения информационной безопасности, Теме 4.1. Средства управления доступом (Аудиторная самостоятельная работа).
Название: Изучение средств управления доступом.
Задание:
1. Изучите средства работы с учетными записями пользователей.
2. Изучите средства разграничения доступа пользователей к файлам и папкам.
3. Изучите программные средства для генерирования и хранения паролей.

Комплект оценочных заданий №4 по Разделу 4. Программно-технические средства обеспечения информационной безопасности, Теме 4.2. Криптографические средства защиты информации (Аудиторная самостоятельная работа).
Название: Изучение методов симметричного шифрования.
Задание:
1. Осуществите шифрование указанного текста методами: простой перестановки, перестановки по маршруту, шифром Цезаря.
2. Осуществите расшифрование указанного текста зашифрованного методом Вижинера.
3. Осуществите расшифрование указанного текста зашифрованного методом гаммирования.

Комплект оценочных заданий №5 по Разделу 4. Программно-технические средства обеспечения информационной безопасности, Теме 4.2. Криптографические средства защиты информации (Аудиторная самостоятельная работа).
Название: Изучение программных средств шифрования информации.
Задание:
1. Изучите стандартные средства шифрования ОС.
2. Изучите возможности средств шифрования программ-архиваторов.
3. Изучите возможности специализированных программ для шифрования данных.
4. Изучите средства создания и проверки контрольных сумм.

Комплект оценочных заданий №6 по Разделу 4. Программно-технические средства обеспечения информационной безопасности, Теме 4.3. Средства защиты от вредоносных программ (Аудиторная самостоятельная работа).
Название: Изучение работы антивирусной программы.
Задание:

1. Изучите возможности встроенного средства антивирусной защиты ОС Windows.
2. Изучите возможности антивирусной утилиты Dr.Web CureIt.
3. Осуществите инсталляцию и настройку антивирусной программы и ее возможности.

Комплект оценочных заданий №7 по Разделу 4. Программно-технические средства обеспечения информационной безопасности, Теме 4.4. Средства резервного копирования (Аудиторная самостоятельная работа).
Название: Изучение средств резервного копирования.
Задание:
1. Изучите возможности стандартных средств резервного копирования ОС.
2. Изучите возможности специализированных средств резервного копирования.
3. Изучите основные методы резервного копирования: полное, дифференциальное, инкрементальное.

Комплект оценочных заданий №8 по Разделу 5. Комплексное обеспечение информационной безопасности, Теме 5.1. Защита информации в персональных компьютерах
(Аудиторная самостоятельная работа).
Название: Изучение средств защиты информации в ПК.
Задание:
Подберите комплекс средств для защиты информации рабочего места пользователя: разграничения доступа, антивирусной защиты, резервного копирования, шифрования, бесперебойности питания, физической защиты и т.д.

Комплект оценочных заданий №9 по Разделу 5. Комплексное обеспечение информационной безопасности, Теме 5.2. Защита информации в компьютерных сетях (Аудиторная самостоятельная работа).
Название: Изучение средств защиты информации в компьютерных сетях.
Задание:
1. Изучите средства межсетевого разграничения.
2. Изучите средства защиты беспроводных сетей.
3. Изучите средства VPN.

4.1.2. ТЕСТОВЫЕ ЗАДАНИЯ
Комплект оценочных заданий №1 по Разделу 1. Угрозы информационной безопасности, Теме 1.1. Основные угрозы и принципы информационной безопасности (Аудиторная самостоятельная работа).

1. Спецификация Банка тестовых заданий по Разделу 1. Угрозы информационной безопасности, Теме 1.1. Основные угрозы и принципы информационной безопасности.

2. Содержание Банка тестовых заданий

Инструкция: выбери правильный(е) ответ(ы).

1. Актуальность и непротиворечивость информации, ее защищенность от РАЗРУШЕНИЯ и НЕСАНКЦИОНИРОВАННОГО ИЗМЕНЕНИЯ, называется …

- конфиденциальностью
+ целостностью

- доступностью

2. Возможность ЗА ПРИЕМЛЕМОЕ ВРЕМЯ получить требуемую информационную услугу, называется …
- конфиденциальностью
- целостностью
+ доступностью

3. Защищенность информации от НЕСАНКЦИОНИРОВАННОГО ДОСТУПА к ней, называется …
+ конфиденциальностью
- целостностью
- доступностью

4. Что из перечисленного относится к основным аспектам информационной безопасности?
+ конфиденциальность
- защищенность
+ целостность
+ доступность

5. Что из перечисленного будет считаться несанкционированным доступом к информации?
- порча информации в результате программного сбоя
+ доступ к информации под чужим логином и паролем
+ кража носителей информации
- блокирование доступа законных пользователей к информации

6. Несанкционированный доступ к информации ведет к нарушению, какого аспекта информационной безопасности?
+ конфиденциальности
- доступности
- целостности

7. Под искажением информации понимают …
- утрату свойств конфиденциальности информации
+ любое преднамеренное или случайное изменение информации
- действие, в результате которого информация перестает физически существовать

8. Под утечкой информации понимают …
+ утрату свойств конфиденциальности информации
- любое преднамеренное или случайное изменение информации
- действие, в результате которого информация перестает физически существовать

9. Под уничтожением информации понимают …
- любое преднамеренное или случайное изменение информации
+ действие, в результате которого информация перестает физически существовать
- преднамеренное действие по созданию ложной информации

10. Под блокированием информации понимают …
- любое преднамеренное или случайное изменение информации
- действие, в результате которого информация перестает физически существовать
+ прекращение или затруднение доступа законных пользователей к информации

11. Под подделкой информации понимают …
- утрату свойств конфиденциальности информации
- любое преднамеренное или случайное изменение информации
+ преднамеренное действие по созданию ложной информации

12. Возможная опасность совершения какого-либо действия против объекта защиты, называется …
+ угрозой
- уязвимостью
- атакой

13. Присущие объекту свойства, приводящие к нарушению безопасности информации, обусловленные недостатками процесса функционирования объекта, называется …
- угрозой
+ уязвимостью
- атакой

14. Чем из перечисленных понятий является ПОПЫТКА РЕАЛИЗАЦИИ угрозы?
- угрозой
- уязвимостью
+ атакой

15. Источники угроз информационной безопасности могут быть …
+ антропогенными
+ техногенными
+ стихийными
- случайными

16. Какие виды источников угроз информационной безопасности могут быть внешними и внутренними?
+ антропогенные
+ техногенные
- стихийные

17. Какой из перечисленных источников угроз относится к ВНЕШНИМ АНТРОПОГЕННЫМ?
+ хакеры
- уборщицы
- системные администраторы
- пользователи

18. Какие из перечисленных источников угроз относятся к ВНУТРЕННИМ АНТРОПОГЕННЫМ?
- хакеры
+ пользователи
+ уборщицы
- пожарные

19. Какой из перечисленных источников угроз относится к ВНЕШНИМ ТЕХНОГЕННЫМ?
- хакеры
- некачественные компьютеры
+ средства связи
- ураганы

20. Какой из перечисленных источников угроз относится к ВНУТРЕННИМ ТЕХНОГЕННЫМ?
- пользователи
- уборщицы
+ некачественные компьютеры
- средства связи

21. Какие из перечисленных источников угроз относятся к СТИХИЙНЫМ?
- хакеры
- пользователи
- уборщицы
+ ураганы
+ пожары

22. Какие виды ущерба могут быть нанесены деловой репутации организации?
+ моральный
+ материальный
- физический

23. Что такое канал утечки информации?
+ физический путь от источника информации к злоумышленнику
- план похищения информации злоумышленником
- канал доступа к сети Интернет

24. Какие из перечисленных каналов утечки информации относятся к ОПТИЧЕСКИМ?
+ подглядывание за изображением на мониторе
+ фотографирование документов или экранов
- подслушивание переговоров сотрудников
- перехват электромагнитных излучений кабелей
- прямое копирование, например на флешку

25. Какие из перечисленных каналов утечки информации относятся к МАТЕРИАЛЬНЫМ?
+ бумажные документы в мусорной корзине

- удаленные файлы в корзине Windows
- электронные подслушивающие закладки («жучки»)
+ утерянные носители информации

26. Как называется канал утечки информации, при котором осуществляется фиксация акустического сигнала при воздействии его на строительные конструкции?
+ виброакустический
- акустоэлектрический
- строительный
- материальный

27. Какое из перечисленных определений наиболее точно характеризует понятие хакер?
+ ИТ-специалист, который понимает самые основы работы компьютерных систем
- любой пользователь, осуществляющий несанкционированный доступ к информации
- человек, осуществляющий взлом защиты лицензионных программных продуктов

28. Кто из перечисленных личностей относится к известным хакерам-взломщикам?
+ Эдвард Сноуден
+ Джулиан Ассандж
+ Кевин Митник
- Билл Гейтс
- Стив Джобс

29. Как называется хакерская атака, осуществляемая при помощи программ или устройств для перехвата и анализа сетевого трафика?
+ сниффинг пакетов
- IP-спуфинг
- PHP-инъекция
- отказ в обслуживании

30. Как называется хакерская атака, когда атакуемый сервер не может обработать огромное количество входящих пакетов?
- социальная инженерия
- IP-спуфинг
- переполнение буфера
+ отказ в обслуживании

31. Чем отличается DDoS атака от DoS атаки?
- атака осуществляется группой хакеров
- атака осуществляется на множество серверов одновременно
+ атака осуществляется с множества компьютеров на один сервер

32. Как называется набор программных средств, обеспечивающих МАСКИРОВКУ объектов при хакерской атаке?
- бэкдур
- троян
+ руткит
- DDoS

33. Как называется метод осуществления несанкционированного доступа к информационным ресурсам, основанный на особенностях психологии человека?

- человек посередине
- отказ в обслуживании
+ социальная инженерия

34. Как называется метод социальной инженерии, при котором жертве по электронной почте отправляется сообщение, подделанное под официальное письмо – от банка или платёжной системы?

- дорожное яблоко
- троянский конь
+ фишинг

35. Как называется метод социальной инженерии, распространенный в общественных местах (кафе, торговых центрах, общественном транспорте) при котором злоумышленник подсматривает информацию на экране жертвы?

- дорожное яблоко
- фишинг
+ плечевой серфинг

36. Как называется метод социальной инженерии, при котором жертва сама предлагает злоумышленнику нужную ему информацию?

- претекстинг
- фишинг
+ обратная социальная инженерия

37. Как называется метод социальной инженерии, при котором злоумышленник подбрасывает инфицированный носитель информации в месте, где носитель может быть легко найден?

- претекстинг
- троянский конь
+ дорожное яблоко

3.Таблица форм тестовых заданий

Всего ТЗ	Из них количество ТЗ в форме			
	закрытых	открытых	на соответствие	на порядок
	шт. %	шт. %	шт. %	шт. %
100%	100	-	-	-

4. Таблица ответов к тестовым заданиям

Верные ответы отмечены знаком « + », неверные отмечены знаком « - ».

Комплект оценочных заданий №2 по Разделу 2. Нормативно-правовые основы информационной безопасности, Теме 2.1. Правовое обеспечение информационной безопасности и Теме 2.2. Стандарты информационной безопасности (Аудиторная самостоятельная работа).

1. Спецификация Банка тестовых заданий по Разделу 2. Нормативно-правовые основы информационной безопасности, Теме 2.1. Правовое обеспечение информационной безопасности и Теме 2.2. Стандарты информационной безопасности.

2. Содержание Банка тестовых заданий

Инструкция: выбери правильный(е) ответ(ы).

1. В каких Российских законодательных актах рассматриваются вопросы информационной безопасности?

- Закон «О защите информации»
- Информационный кодекс РФ
+ Уголовный кодекс РФ
+ Закон «Об авторском праве»
+ Закон «Об электронной подписи»
+ Закон «Об информации, информационных технологиях и о защите информации»

2. Какой законодательный акт ГАРАНТИРУЕТ гражданину ПРАВО свободно искать, получать, передавать, производить и распространять информацию любым законным способом?

- Закон «О защите информации»
+ Конституция РФ
- Уголовный кодекс РФ

3. В каких Российских законодательных актах рассматриваются вопросы ОТВЕТСТВЕННОСТИ в области информационной безопасности?

+ Закон «Об информации, информационных технологиях и о защите информации»
- Конституция РФ
+ Уголовный кодекс РФ

4. За какие виды преступлений в области информационной безопасности предусмотрены НАКАЗАНИЯ в Уголовном кодексе РФ?

+ неправомерный доступ к компьютерной информации
+ создание, использование и распространение вредоносных программ
+ нарушение правил эксплуатации ЭВМ
- использование контрафактной продукции

5. За какие виды преступлений в области информационной безопасности в Уголовном кодексе РФ предусмотрено ЛИШЕНИЕ СВОБОДЫ?

+ неправомерный доступ к компьютерной информации
+ создание, использование и распространение вредоносных программ
+ нарушение правил эксплуатации ЭВМ
- использование контрафактной продукции

6. За какое преступление в области информационной безопасности Уголовный кодекс РФ предусматривает САМОЕ СУРОВОЕ НАКАЗАНИЕ, лишение свободы на срок до семи лет?

- нарушение правил эксплуатации ЭВМ
- неправомерный доступ к компьютерной информации
+ создание, использование и распространение вредоносных программ

7. К какому классу относятся стандарты, регламентирующие различные аспекты реализации и использования средств и методов защиты?
- оценочные
+ спецификации

8. К какому классу относятся стандарты, предназначенные для оценки и классификации информационных систем и средств защиты по требованиям безопасности?
+ оценочные
- спецификации

9. Какой из перечисленных стандартов РФ, является наиболее полным на данный момент и называется также «Общие критерии оценки безопасности информационных технологий»?
- ГОСТ Р 50922-96 Защита информации. Основные термины и определения.
- ГОСТ Р 51275-99 Защита информации. Объект информатизации
+ ГОСТ Р ИСО/МЭК 15408 Методы и средства обеспечения безопасности

10. Какие из перечисленных стандартов являются Российскими?
+ ГОСТ Р 50922-96
+ Р 50.1.053-2005
+ ГОСТ Р ИСО/МЭК 15408
- BS 7799-1:2005
- «Оранжевая книга»

11. Какая международная организация занимается разработкой стандартов информационной безопасности?
- ГОСТ
- AES
+ ISO
- BS

12. Кто является разработчиком стандарта BS 7799-1:2005 «Практические правила управления информационной безопасностью»?
- Россия
- США
+ Великобритания
- Международная организация по стандартизации

13. Кто является разработчиком стандарта ISO/IEC 17799:2005 – «Информационные технологии – Технологии безопасности – Практические правила менеджмента информационной безопасности»?
- Россия
- Великобритания
+ Международная организация по стандартизации

14. Как официально называется стандарт, обычно упоминаемый как «Оранжевая книга»?
- Критерии безопасности информационных систем

+ Критерии оценки доверенных компьютерных систем
- Критерии оценки информационных систем

15. Выбери верные ответы:
+ Оранжевая книга является прародителем многих национальных стандартов безопасности ИС
+ Оранжевая книга оценивает степень доверия к ИС в зависимости от используемой в ИС модели управления доступом
+ Оранжевая книга разработана в США
- Оранжевая книга является Британским стандартом

16. Какой класс безопасности компьютерных систем по «Оранжевой книге» обеспечивает НАИБОЛЬШЕЕ ДОВЕРИЕ (обеспечивает лучшую защищенность ИС)?
+ уровень A
- уровень B
- уровень C
- уровень D
- уровень E

17. Какой класс безопасности компьютерных систем по «Оранжевой книге» обеспечивает НАИМЕНЬШИЙ ДОВЕРИЕ (обеспечивает худшую защищенность ИС)?
- уровень A
- уровень B
- уровень C
+ уровень D
- уровень E

18. Как называется уровень C согласно «Оранжевой книге»?
- неудовлетворительный уровень безопасности
- принудительное управление доступом
+ произвольное управление доступом

19. Как называется уровень A согласно «Оранжевой книге»?
+ верифицируемая безопасность
- неудовлетворительный уровень безопасности
- принудительное управление доступом

20. Как называется уровень D согласно «Оранжевой книге»?
- верифицируемая безопасность
+ неудовлетворительный уровень безопасности
- произвольное управление доступом

3.Таблица форм тестовых заданий

Всего ТЗ	Из них количество ТЗ в форме			
	закрытых	открытых	на соответствие	на порядок
	шт. %	шт. %	шт. %	шт. %
100%	100	-	-	-

4. Таблица ответов к тестовым заданиям

Верные ответы отмечены знаком « + », неверные отмечены знаком « - ».

Комплект оценочных заданий №3 по Разделу 3. Организационно-технические и режимные методы обеспечения информационной безопасности, Теме 3.1. Административный уровень информационной безопасности и Теме 3.2. Процедурный уровень информационной безопасности (Аудиторная самостоятельная работа).

1. Спецификация Банка тестовых заданий по Разделу 3. Организационно-технические и режимные методы обеспечения информационной безопасности, Теме 3.1. Административный уровень информационной безопасности и Теме 3.2. Процедурный уровень информационной безопасности.

2. Содержание Банка тестовых заданий

Инструкция: выбери правильный(е) ответ(ы).

1. К уровню обеспечения информационной безопасности предприятия относится Политика информационной безопасности?

+ административный
- программно-технический
- нормативно-правовой

2. Что из перечисленного можно считать эффективной Политикой информационной безопасности предприятия?

+ совокупность нормативных документов, инструкций, регламентов, процедур и т.п. в области информационной безопасности
- комплект инструкций для пользователей
- пакет документов на тему информационной безопасности

3. Каким способом лучше создавать эффективную Политику информационной безопасности?

+ разработать самостоятельно
- взять готовую в сети Интернет
- использовать соответствующий ГОСТ

4. Как называется раздел Политики информационной безопасности, подтверждающий заинтересованность высшего руководства организации проблемами информационной безопасности?

+ вводный раздел
- раздел управления
- юридический раздел
- раздел физической защиты

5. Как называется раздел Политики информационной безопасности, описывающий подход к управлению компьютерами и сетями передачи данных?

- вводный раздел
+ раздел управления
- юридический раздел
- раздел физической защиты

6. Как называется раздел Политики информационной безопасности, подтверждающий соответствие политики информационной безопасности текущему законодательству?
- вводный раздел
- раздел управления
+ юридический раздел
- раздел физической защиты

7. В каком разделе Политики информационной безопасности могут быть описаны типы помещений организации и необходимые для них меры безопасности?
- вводный раздел
- раздел управления
- юридический раздел
+ раздел физической защиты

8. Что из перечисленного относится к принципам управления персоналом?
+ минимизация привилегий
+ разделение обязанностей
- разделение привилегий
- максимизация обязанностей

9. Выделение пользователям только тех прав доступа, которые необходимы им для выполнения служебных обязанностей, называется – …
+ минимизацией привилегий
- разделением обязанностей
- минимизацией обязанностей
- разделением привилегий

10. Распределение ролей и ответственности, так чтобы один человек не мог нарушить критически важный для организации процесс, называется – …
- минимизацией привилегий
+ разделением обязанностей
- минимизацией обязанностей
- разделением привилегий

11. В каких случаях необходимо ликвидировать права доступа пользователя?
+ при увольнении сотрудника
- при нахождении сотрудника в отпуске
+ при смене должности сотрудником
- при получении выговора сотрудником

12. В какой момент начинается управление персоналом?
- при подборе кандидатов на новую должность
+ при составлении описания новой должности
- при приеме на работу нового сотрудника
- с первого рабочего дня нового сотрудника

13. При увольнении сотрудника с точки зрения информационной безопасности, необходимо:

+ принять все пароли
+ принять оборудование
+ ликвидировать права доступа уволенного
- форматировать все устройства хранения информации, которыми пользовался сотрудник

14. В каком месте организации должна находиться серверная комната с точки зрения информационной безопасности?
+ вдали от основного потока посетителей
- точно в географическом центре организации
- ближе к главному входу в здание
- ближе к кабинету руководителя организации

15. Как необходимо обозначить серверную комнату на различных указателях и настенных картах в организации с точки зрения информационной безопасности?
+ обозначать не стоит
- серверная комната
- информационный центр

16. Что из перечисленного можно использовать в качестве электронных систем обнаружения злоумышленников?
+ охранную сигнализацию
- кодовые замки
+ камеры видеонаблюдения
- межсетевые экраны

17. Какой тип замка может позволять устанавливать различные комбинации для каждого пользователя и вести журнал событий регистрации пользователей?
+ электронный кодовый
- механический кодовый
- любой кодовый

18. Какие типы датчиков используются для физической защиты серверной комнаты?
+ пожарные
+ охранные
+ протечки воды
- обрыва кабеля питания

19. Какие бывают типы пожарных датчиков?
+ дымовые
+ тепловые
- контактные
- ёмкостные

20. Что из перечисленного относится к охранной сигнализации?
+ емкостные датчики
+ датчики движения
+ инфракрасные (лазерные) датчики
+ вибрационные датчики

- дымовые датчики

21. Что из перечисленного относится к пожарной сигнализации?
- емкостные датчики
+ тепловые датчики
- датчики протечки
- вибрационные датчики
+ дымовые датчики

22. Что из перечисленного относится к средствам защиты кабельной системы сети?
- охранные датчики
+ кабель-каналы
+ герметичные полиэтиленовые рукава
- камеры наблюдения

23. Какую систему пожаротушения предпочтительнее использовать в серверных комнатах?
- пенную
+ газовую
- порошковую

24. Какой вариант настройки защиты в BIOS достаточен для защиты компьютера от несанкционированного доступа?
- пароль на вход в BIOS
- пароль на вход в систему
+ оба пароля

25. Что представляет собой комната ИТ-безопасности?
+ модульная конструкция типа помещение в помещении
- кабинет обучения информационной безопасности
- помещение, в котором обеспечена защита от прослушивания

3.Таблица форм тестовых заданий

Всего ТЗ	Из них количество ТЗ в форме			
	закрытых	открытых	на соответствие	на порядок
	шт. %	шт. %	шт. %	шт. %
100%	100	-	-	-

4. Таблица ответов к тестовым заданиям

Верные ответы отмечены знаком « + », неверные отмечены знаком « - ».

Комплект оценочных заданий №4 по Разделу 4. Программно-технические средства обеспечения информационной безопасности, Теме 4.1. Средства управления доступом (Аудиторная самостоятельная работа).

1. Спецификация Банка тестовых заданий по Разделу 4. Программно-технические средства обеспечения информационной безопасности, Теме 4.1. Средства управления доступом.

2. Содержание Банка тестовых заданий

Инструкция: выбери правильный(е) ответ(ы).

1. Лицо или процесс, действие которого регламентируются правилами разграничения доступа, называется …

+ субъектом
- объектом
- клиентом
- пользователем

2. Единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа, называется …

- субъектом
+ объектом
- клиентом
- файлом

3. Как еще называется мандатное управление доступом?

+ принудительное
- произвольное
- ролевое
- избирательное

4. Как еще называется произвольное управление доступом?

- мандатное
+ дискреционное
+ избирательное

5. В какой модели управления доступом применяются списки или матрицы доступа?

- мандатной
+ дискреционной
- ролевой
- любой

6. В какой модели управления доступом применяются метки безопасности (конфиденциальности)?

+ мандатной
- дискреционной
- ролевой
- любой

7. Что описывает метка безопасности субъекта в принудительной модели управления доступом?

+ его благонадежность
- степень его конфиденциальности
- его права доступа
- его роль

8. Кто устанавливает права доступа к конкретному объекту в ДИСКРЕЦИОННОЙ модели управления доступом?
- любой пользователь
- только системный администратор
+ владелец объекта
- сама система

9. Кто устанавливает права доступа к конкретному объекту в МАНДАТНОЙ модели управления доступом?
- любой пользователь
- только системный администратор
- владелец объекта
+ сама система

10. Кому, согласно дискреционной модели управления доступом, субъект с определенным правом доступа может передать это право?
- ни кому
- только системному администратору
+ любому другому субъекту

11. В какой модели управления доступом пользователь сам устанавливает права доступа к объектам, чьими владельцем является?
+ дискреционной
- мандатной
- ролевой
- любой

12. Закрытая система дискреционного управления доступом подразумевает, что изначально …
+ объект не доступен никому, и в списке прав доступа описывается список разрешений
- объект доступен всем, и в списке прав доступа описывается список ограничений

13. Открытая система дискреционного управления доступом подразумевает, что изначально …
- объект не доступен никому, и в списке прав доступа описывается список разрешений
+ объект доступен всем, и в списке прав доступа описывается список ограничений

14. Основными преимуществами произвольного управления доступом являются …
+ простота реализации
- простота администрирования
- высокая степень безопасности
+ гибкость

15. Основным преимуществом принудительного управления доступом является …
- простота реализации
- простота администрирования
+ высокая степень безопасности
- гибкость

16. Какая модель управления доступом применяется в операционных системах Microsoft Windows?
- мандатная
+ дискреционная
- ролевая

17. В мандатной модели объекту присвоена метка безопасности «конфиденциально», категория «бухгалтерия». Какие СУБЪЕКТЫ могут иметь доступ к данному объекту?
+ секретно, бухгалтер
+ конфиденциально, бухгалтер
- совершенно секретно, инженер
- любые субъекты

18. В мандатной модели объекту присвоена метка безопасности «несекретно», категория «кадры». Какой СУБЪЕКТ будет иметь доступ к данному объекту?
- только секретно, кадры
- только секретно, бухгалтер
- только несекретно, инженер
+ все субъекты

19. В мандатной модели субъект имеет уровень доступа «секретно», категория «бухгалтер». Какие ОБЪЕКТЫ будут ему доступны?
- совершенно секретно, бухгалтерия
+ секретно, бухгалтерия
+ конфиденциально, бухгалтерия
+ несекретно, кадры
- секретно, кадры

20. Что из перечисленного понимаете под термином протоколирование?
- анализ накопленной информации
+ сбор и накопление информации о *событиях*, происходящих в информационной системе
- процесс записи информации о происходящих с каким-то объектом событиях в журнал

21. Что из перечисленного понимаете под термином журналирование?
- анализ накопленной информации
- сбор и накопление информации о *событиях*, происходящих в информационной системе
+ процесс записи информации о происходящих с каким-то объектом событиях в журнал

22. Что из перечисленного понимаете под термином аудит?
+ анализ накопленной информации
- сбор и накопление информации о *событиях*, происходящих в информационной системе
- процесс записи информации о происходящих с каким-то объектом событиях в журнал

23. Какие задачи можно решать при помощи протоколирования и аудита?
+ обеспечение подотчетности пользователей
+ обеспечение подотчетности администраторов
+ возможность реконструкции последовательности событий

+ обнаружение попыток нарушений информационной безопасности
- обеспечение аутентификации

24. Оперативный аудит с АВТОМАТИЧЕСКИМ реагированием на выявленные нештатные ситуации, называется …
+ активным
- оперативным
- автоматическим

25. В активном аудите к ошибкам первого рода относится?
+ пропуск атаки
- ложное срабатывание

26. В активном аудите к ошибкам второго рода относится?
- пропуск атаки
+ ложное срабатывание

27. Действия, выполняемые в рамках имеющихся полномочий, но нарушающие политику безопасности, называются – …
- присвоением полномочий
+ злоупотреблением полномочиями
- нарушением полномочий

28. Какие из перечисленных файловых систем относятся к журналируемым?
+ NFS+
+ NTFS
- FAT32
+ ext3fs
- ext2fs

29. Процесс сообщения субъектом своего имени или номера, с целью отличить данный субъект от других субъектов, называется – …
- авторизацией
- аутентификацией
+ идентификацией

30. Предоставление субъекту некоторых прав и проверка их наличия, называется – …
+ авторизацией
- аутентификацией
- идентификацией

31. Процедура проверки соответствия субъекта и того, за кого он пытается себя выдать, с помощью некой уникальной информации, называется – …
- авторизацией
+ аутентификацией
- идентификацией

32. Что из перечисленного может быть «двухсторонним»?

- авторизация
+ аутентификация
- идентификация

33. К какому виду аутентификационных сущностей относятся пароли?
- нечто, чем владеет субъект
+ нечто, что знает субъект
- нечто, что является частью субъекта

34. К какому виду аутентификационных сущностей относится USB-ключ?
+ нечто, чем владеет субъект
- нечто, что знает субъект
- нечто, что является частью субъекта

35. К какому виду аутентификационных сущностей относятся отпечатки пальцев?
- нечто, чем владеет субъект
- нечто, что знает субъект
+ нечто, что является частью субъекта

36. К какому виду аутентификационных сущностей относится сетчатка глаза?
- нечто, чем владеет субъект
- нечто, что знает субъект
+ нечто, что является частью субъекта

37. Что из перечисленного относится к ФИЗИОЛОГИЧЕСКИМ биометрическим характеристикам?
- голос
+ отпечатки пальцев
- почерк субъекта
+ сетчатка глаза
+ форма кисти руки

38. Что из перечисленного относится к ПОВЕДЕНЧЕСКИМ биометрическим характеристикам?
+ голос
- отпечатки пальцев
+ почерк субъекта
- сетчатка глаза
- форма кисти руки

39. Выбери два верных утверждения.
+ ввод пароля можно подсмотреть
+ главное достоинство парольной аутентификации – простота и привычность
- пароль невозможно подобрать
- парольная аутентификация обладает очень высокой надежностью

40. Что из перечисленного применяется для повышения надежности парольной аутентификации?

- использование единого пароля для всех сервисов
+ использование одноразовых паролей
+ ограничение числа неудачных попыток ввода
+ периодическая смена паролей

41. Какие из приведенных примеров паролей МОЖНО считать надежными?
+ g1f2h3j4k5m6
- c1$d
- Иван Иванович
+ y&7h2*sv

42. Почему пароль типа «c1$d» считается НЕ надежным?
+ слишком короткий
- используются цифры
- не используются символы кириллицы

43. Почему пароль типа «Иван Иванович» считается НЕ надежным?
- слишком короткий
+ не используются цифры
+ не используются спецсимволы
+ используется осмысленный набор символов

44. Какие из приведенных примеров паролей НЕЛЬЗЯ считать надежными?
+ 1234567890
- g1f2h3j4k5m6
- y&7h2*sv
+ Password

45. Какой метод парольной аутентификации более надежен?
+ на основе одноразовых паролей
- на основе многоразовых паролей

46. Идентификация, аутентификация. Выбери верный ответ. Что представляет собой программный продукт Kerberos?
+ сервер аутентификации
- сервер идентификация
- центр авторизации

47. Происходит ли при использовании программного продукта Kerberos передача паролей по сети?
+ нет
- да

48. Что из перечисленного относится к средствам идентификации?
+ Штрих-код
+ RFID
+ Биометрия
- Пароль

49. Что из перечисленного относится к средствам аутентификации?
- Штрих-код
- RFID
+ Биометрия
+ Пароль

3.Таблица форм тестовых заданий

Всего ТЗ	Из них количество ТЗ в форме			
	закрытых	открытых	на соответствие	на порядок
	шт. %	шт. %	шт. %	шт. %
100%	100	-	-	-

4. Таблица ответов к тестовым заданиям

Верные ответы отмечены знаком « + », неверные отмечены знаком « - ».

Комплект оценочных заданий №5 по Разделу 4. Программно-технические средства обеспечения информационной безопасности, Теме 4.2. Криптографические средства защиты информации (Аудиторная самостоятельная работа).

1. Спецификация Банка тестовых заданий по Разделу 4. Программно-технические средства обеспечения информационной безопасности, Теме 4.2. Криптографические средства защиты информации.

2. Содержание Банка тестовых заданий

Инструкция: выбери правильный(е) ответ(ы).

1. Исследование возможности дешифрования информации БЕЗ ЗНАНИЯ КЛЮЧЕЙ, называется …

+ криптоанализом
- криптологией
- криптостойкостью

2. Какое понятие включает в себя другие два?
- криптоанализ
- криптография
+ криптология

3. Процесс извлечения открытого текста БЕЗ ЗНАНИЯ криптографического ключа на основе известного шифрованного текста, называется …

- расшифрованием
- криптологией
+ дешифрованием

4. Процесс извлечения открытого текста из зашифрованного с использованием криптографического ключа, называется …

+ расшифрованием
- криптологией
- дешифрованием

5. Какой метод шифрования использовал Юлий Цезарь?
- шифрование гаммированием
+ шифрование заменой
- шифрование перестановкой

6. Самый древний шифрованный текст, найденный в Месопотамии, содержит информацию …
- о рецепте бальзамирования тела фараона
- о рецепте бессмертия
+ о рецепте глазури для гончарных изделий

7. В Древней Греции по сведениям Плутарха использовалось шифрующее устройство – скиталь, которое представляло собой …
- конус
+ цилиндр
- шар

8. Криптографические методы, использующие и для шифрования, и для дешифрования ОДИН И ТОТ ЖЕ КЛЮЧ, называются …
- методами асимметричного шифрования
+ методами симметричного шифрования

9. При симметричном шифровании сообщение шифруется при помощи …
- двух ключей
+ закрытого ключа
+ одного и того же ключа
- открытого ключа

10. К каким методам относится шифрование по таблице Виженера?
- ассиметричным
+ симметричным
- и тем и другим

11. Что из перечисленного относится к методам симметричного шифрования?
+ шифрование гаммированием
+ шифрование заменой
+ шифрование перестановкой
- шифрование с открытым ключом

12. Как называется шифрование заменой, при которой используется несколько алфавитов?
- монофоническое
+ полиалфавитное
- многоконтурное

13. Как называется шифрование заменой, при которой для редко встречающихся символов применяют один алфавит, а для часто встречающихся – несколько?
+ монофоническое
- полиалфавитное

- многоконтурное

14. К какому методу относится шифрование по таблице Виженера?
- шифрование гаммированием
+ шифрование заменой
- шифрование перестановкой

15. Правило логической ЭКВИВАЛЕНТНОСТИ гласит: при сложении двух одинаковых символов получаем …
- логическую единицу
+ логический ноль

16. Шифрование с использованием в качестве гаммы словосочетания «автоматизированные информационные системы», относится к гаммированию с …
- бесконечной гаммой
+ конечной длинной гаммой
- конечной короткой гаммой

17. Шифрование с использованием в качестве гаммы числа Пи, относится к гаммированию с …
+ бесконечной гаммой
- конечной длинной гаммой
- конечной короткой гаммой

18. Криптографические методы, использующие и для шифрования, и для дешифрования два разных ключа, один из которых закрытый, другой открытый, называются …
+ методами асимметричного шифрования
- методами симметричного шифрования

19. При асимметричном ШИФРОВАНИИ сообщение шифруется при помощи …
- закрытого ключа
- одного и того же ключа
+ открытого ключа

20. При асимметричном ШИФРОВАНИИ сообщение расшифровывается при помощи …
- без ключей
+ закрытого ключа
- открытого ключа

21. Что из перечисленного относится к методам асимметричного шифрования?
- шифрование гаммированием
- шифрование заменой
+ шифрование с открытым ключом

22. Какие называются математические функции, лежащие в основе ассиметричного шифрования?
+ односторонние
- ассиметричные

- бесконечные

23. Электронная цифровая подпись (ЭЦП) представляет собой:
- цифровое изображение подписи автора
+ последовательность из нескольких символов в электронном документе
- полный текст в зашифрованном виде, добавленный к файлу с защищаемым текстом

24. Выбери верное понятие электронной цифровой подписи (ЭЦП):
+ ЭЦП — это реквизит ЭЛЕКТРОННОГО документа, предназначенный для удостоверения источника данных и защиты данного электронного документа от ПОДДЕЛКИ
- ЭЦП — это реквизит БУМАЖНОГО документа, предназначенный для удостоверения источника данных и защиты данного электронного документа от ПОДДЕЛКИ
- ЭЦП — это реквизит ЭЛЕКТРОННОГО документа, предназначенный для удостоверения источника данных и защиты данного электронного документа от НЕСАНКЦИОНИРОВАННОГО ИСПОЛЬЗОВАНИЯ

25. Преобразование входного массива данных произвольной длины в выходную битовую строку фиксированной длины, называется …
+ хэшированием
- ЭЦП
- кодированием

26. Электронная цифровая подпись (ЭЦП) обеспечивает:
+ удостоверение источника документа
+ защиту от изменений документа
- защиту от несанкционированного использования
+ невозможность отказа от авторства

27. Для создания ЭЦП используется …
+ закрытый ключ
- открытый ключ

28. При проверке ЭЦП используется …
- оба ключа
- закрытый ключ
+ открытый ключ

29. Какие из перечисленных алгоритмов шифрования предназначены для создания хеш-функций?
- DES
+ MD5
+ SHA
- AES

30. Какие из перечисленных алгоритмов шифрования используются для электронной цифровой подписи (ЭЦП)?
- DES

+ RSA
+ DSA
- AES

31. Какие из перечисленных алгоритмов относятся к симметричным?
+ DES
- RSA
+ AES
- MD5

32. Какие из перечисленных алгоритмов относятся к асимметричным?
+ RSA
+ DSA
- AES
+ MD5

33. Какой из перечисленных алгоритмов часто используется в Интернете для вычисления контрольных сумм?
- DES
+ MD5
- SHA
- AES

34. Какой из перечисленных алгоритмов часто используется для защиты информации в беспроводных сетях Wi-Fi?
- MD5
- RSA
+ AES

35. Какие из перечисленных алгоритмов шифрования НЕ МОГУТ использоваться в Российских государственных учреждениях?
- ГОСТ Р 34.10-2001
+ MD5
+ SHA
+ IDEA
+ AES

36. Какие из перечисленных средств шифрования можно отнести к АППАРАТНЫМ?
- ЭЦП
+ шифровальная машина Enigma
- программа 7-Zip
+ скиталь
- AES128

37. Современные средства криптографической защиты информации подразделяются на следующих два вида …
- аппаратные
+ аппаратно-программные

+ программные

38. Каковы достоинства ассиметричных алгоритмов шифрования?
- короткие ключи шифрования
+ высокая криптостойкость
+ отсутствие проблемы передачи ключа второй стороне
- высокая скорость шифрования

3.Таблица форм тестовых заданий

Всего ТЗ	Из них количество ТЗ в форме			
	закрытых	открытых	на соответствие	на порядок
	шт. %	шт. %	шт. %	шт. %
100%	100	-	-	-

4. Таблица ответов к тестовым заданиям

Верные ответы отмечены знаком « + », неверные отмечены знаком « - ».

Комплект оценочных заданий №6 по Разделу 4. Программно-технические средства обеспечения информационной безопасности, Теме 4.3. Средства защиты от вредоносных программ (Аудиторная самостоятельная работа).

1. Спецификация Банка тестовых заданий по Разделу 4. Программно-технические средства обеспечения информационной безопасности, Теме 4.3. Средства защиты от вредоносных программ.

2. Содержание Банка тестовых заданий

Инструкция: выбери правильный(е) ответ(ы).

1. Каким еще термином обозначают вредоносные программы?
- Virusware
- Freeware
+ Malware

2. Что из перечисленного относится к вредоносным программам?
+ Backdoor-утилиты
- Backup-утилиты
+ Сетевые черви
+ Троянские программы

3. Какие из перечисленных вредоносных программ относятся к вирусам?
+ Virus.Win9x.CIH
+ Macro.Word97.Thus
- Net-Worm.Win32.Sasser
- Trojan-Spy.Win32.Small.b

4. Какие из перечисленных вредоносных программ относятся к сетевым червям?
- Virus.Win9x.CIH
+ Net-Worm.Win32.Sasser
+ Email-Worm.Win32.Netsky.q
- Backdoor.Win32.Netbus.170

5. Какие из перечисленных вредоносных программ относятся к троянским программам?
- Virus.Win9x.CIH
- Email-Worm.Win32.Netsky.q
+ Trojan-Spy.Win32.Small.b
+ Backdoor.Win32.Netbus.170

6. Выбери верные варианты ответов:
+ вредоносные программы способны заразить файлы на flash-карте при её чтении
- вредоносные программы способны заразить файлы на оптическом диске при его чтении
+ вредоносные программы способны стереть информацию на жестком диске

7. Как называется программа, распространяющаяся по сетевым каналам, способная к автономному преодолению систем защиты, а также к созданию и дальнейшему распространению своих копий?
- Вирус
+ Сетевой червь
- Троянская программа

8. Как называется программа, способная создавать свои копии и внедрять их в файлы, системные области компьютера, а также осуществлять иные деструктивные действия?
+ Вирус
- Сетевой червь
- Троянская программа

9. Как называется программа, отличающаяся отсутствием механизма создания собственных копий и проникающая в компьютер под видом полезных программ?
- Вирус
- Сетевой червь
+ Троянская программа

10. Какие виды вредоносных программ создают свои вирусные копии в зараженном компьютере?
+ Вирусы
+ Сетевые черви
- Троянские программы

11. По способу подготовки своих копий вирусы бывают:
- Загрузочные
+ Метаморфные
+ Полиморфные
- Резидентные

12. По способу активации (объектам заражения) вирусы бывают:
+ Загрузочные
+ Макро
+ Файловые
- Полиморфные

- Резидентные

13. По способу заражения вирусы бывают:
- Метаморфные
+ Резидентные
+ Нерезидентные
- Файловые

14. Какие типы файлов способны заразить файловые вирусы?
+ exe
+ dll
- avi
- doc

15. Какие типы файлов способны заразить макровирусы?
- exe
+ xls
+ doc
- txt

16. Какие типы файлов способны заразить скрипт-вирусы?
- exe
- doc
+ vbs
+ js

17. Вирусы, какого вида постоянно находятся в оперативной памяти компьютера?
+ резидентные
- нерезидентные
18. Какие из перечисленных видов червей бывают?
+ P2P
- Загрузочные
+ Почтовые
+ Сетевые
- Файловые

19. По выполняемым функциям троянские программы бывают:
+ Клавиатурные шпионы
+ Вымогатели
+ Похитители паролей
- Мониторные шпионы
+ Модификаторы настроек браузера

20. Какие способы проникновения в компьютер используют троянские программы?
+ Кооперация
+ Маскировка
- Полиморфизм
- Сканирование портов

21. Что из перечисленного может являться причинами проникновения вредоносных программ в компьютер с установленной антивирусной программой?
+ Антивирус отключен
+ Вирус еще не известен антивирусу
- Используется бесплатный антивирус
+ Устаревшие антивирусные базы

22. Что из перечисленного относится к ЯВНЫМ признакам присутствия вредоносных программ в компьютере?
+ Всплывающие сообщения
+ Изменение настроек браузера
- Незнакомые процессы в памяти
+ Несанкционированный дозвон в Интернет

23. Что из перечисленного относится к КОСВЕННЫМ признакам присутствия вредоносных программ в компьютере?
+ Блокирование антивируса
+ Блокирование антивирусных сайтов
- Изменение настроек браузера
- Незнакомые процессы в памяти

24. Что из перечисленного относится к СКРЫТЫМ признакам присутствия вредоносных программ в компьютере?
- Блокирование антивирусных сайтов
+ Незнакомые процессы в памяти
+ Необычная сетевая активность
- Несанкционированный дозвон в Интернет

25. Где следует искать проявления присутствия вирусов в системе?
+ диспетчер задач
- панель управления
+ системный реестр
+ автозагрузка

26. Что из перечисленного может являться причинами проникновения вредоносных программ в компьютер с установленной антивирусной программой?
+ Антивирус отключен пользователем
+ Новая вредоносная программа, еще не известная антивирусу
- Используется бесплатный антивирус
+ Устаревшие антивирусные базы

27. Что из перечисленного относится к организационным методам защиты от вредоносных программ?
+ Не открывать почтовые сообщения от незнакомых отправителей
+ Проверять на наличие вирусов файлы, загружаемые из сети Интернет
- Использовать брандмауэры
- Устанавливать обновления операционной системы

+ Регулярно обновлять антивирусные базы

28. Что из перечисленного относится к техническим методам защиты от вредоносных программ?
- Не открывать почтовые сообщения от незнакомых отправителей
+ Использовать брандмауэры
- Регулярно обновлять антивирусные базы
+ Устанавливать обновления прикладных программ
+ Устанавливать обновления операционной системы
+ Использовать антиспам-фильтры

29. Как называется класс программ, предназначенный для борьбы с вредоносными программами?
- Файерволл
+ Антивирус
- Антивредонос

30. Технология обнаружения вредоносных программ, основанная на нахождении, уникальная последовательности байт, присутствующей в данном вирусе и не встречающейся в других программах называется – …
+ Сигнатурным анализом
- Вероятностным анализом
- Эмуляционным анализом

31. Какие технологии относятся к так называемой проактивной защите?
+ Поведенческий анализ
- Сигнатурный анализ
+ Песочница
+ Эвристический анализ

32. Технология обнаружения вредоносных программ, основанная на выявлении подозрительных объектов, называется – …
- Сигнатурным анализом
+ Вероятностным анализом
- Эмуляционным анализом

33. Что из перечисленного способен произвести антивирус с найденной вредоносной программой, используя СИГНАТУРНЫЕ методы обнаружения?
- Выдать сообщение о наличие подозрительного объекта
+ Отправить файл в карантин
+ Попытаться вылечить файл
+ Удалить инфицированный файл

34. Что из перечисленного способен произвести антивирус с найденной вредоносной программой, используя ВЕРОЯТНОСТНЫЕ методы обнаружения?
+ Выдать сообщение о наличие подозрительного объекта
- Отправить файл в карантин
- Попытаться вылечить файл

- Удалить инфицированный файл

35. Какой вид антивирусов запоминает состояние файловой системы, что делает в дальнейшем возможным анализ изменений?
+ Ревизор
- Сканер
- Монитор

36. Что входит в минимальный набор возможностей обычного антивируса?
- Брандмауэр
+ Модуль обновления антивирусной базы
+ Монитор
+ Сканер
- Проактивная защита

37. Какой модуль антивирусной программы проверяет все файлы и процессы, находящиеся в оперативной памяти?
- Модуль обновления антивирусной базы
+ Монитор
- Сканер
- Брандмауэр

38. Какой модуль антивирусной программы проводит полную проверку файлов хранящихся на всех носителях информации?
- Антихакер
- Монитор
+ Сканер
- Брандмауэр

39. Чем отличается облачный антивирус от обычного?
- Не умеет лечить зараженные файлы
+ Не требуется обновлять антивирусные базы
+ Функционирует только при наличии подключения к сети Интернет
+ Антивирусная база находится в Интернете

40. Чем отличается антивирусная утилита Dr.Web CureIt от обычного антивируса?
- Не умеет лечить зараженные файлы
+ Не позволяет обновлять антивирусные базы
+ Не требует установки
+ Не конфликтует с другими антивирусами

41. Какие из перечисленных антивирусных программ бесплатные или имеют бесплатные версии?
+ Avira
- Panda
- Eset NOD32
+ Avast
- Антивирус Касперского

42. Какие из перечисленных антивирусных программ относятся к отечественным?
- Avira
+ Dr.Web
- Eset NOD32
- Avast
+ Антивирус Касперского

43. Какая из перечисленных антивирусных программ распространяется с открытым исходным кодом?
+ ClamAV
- Avira
- Windows Defender
- Avast
- нет верного ответа

44. Какая из перечисленных антивирусных программ входит в состав современных версий ОС Windows?
- Windows ClamAV
- Windows Antivirus
+ Windows Defender

3.Таблица форм тестовых заданий

Всего ТЗ	Из них количество ТЗ в форме			
	закрытых	открытых	на соответствие	на порядок
	шт. %	шт. %	шт. %	шт. %
100%	100	-	-	-

4. Таблица ответов к тестовым заданиям

Верные ответы отмечены знаком « + », неверные отмечены знаком « - ».

Комплект оценочных заданий №7 по Разделу 4. Программно-технические средства обеспечения информационной безопасности, Теме 4.4. Средства резервного копирования (Аудиторная самостоятельная работа).

1. Спецификация Банка тестовых заданий по Разделу 4. Программно-технические средства обеспечения информационной безопасности, Теме 4.4. Средства резервного копирования.

2. Содержание Банка тестовых заданий

Инструкция: выбери правильный(е) ответ(ы).

1. Каким еще термином обозначается резервное копирование?
+ Backup
- Background
- Backdoor
- I’ll be back

2. При каком виде резервного копирования создается первая копия полная, вторая – отличие от первой, третья снова полная и т.д.?

+ дифференциальном
- инкрементальном
- интегральном

3. При каком виде резервного копирования создается первая копия полная, вторая – отличие от первой, третья – отличие от второй и т.д.?
- дифференциальном
+ инкрементальном
- интегральном

4. Какой вид резервного копирования занимает БОЛЬШЕ всего места на носителях информации?
- дифференциальный
+ полный
- инкрементальный

5. Какой вид резервного копирования самый ЭКОНОМНЫЙ с точки зрения занимаемого места на носителях информации?
- дифференциальный
- полный
+ инкрементальный

6. Какой вид резервного копирования требует НАИБОЛЬШЕЕ количество времени на создание резервных копий?
- дифференциальный
+ полный
- инкрементальный

7. Какой вид резервного копирования требует НАИМЕНЬШЕЕ количество времени на создание резервных копий?
- дифференциальный
- полный
+ инкрементальный

8. Как называется вид резервного копирования, при котором создается своеобразный «снимок» жесткого диска и копируется на носитель сектор за сектором?
- клонирование
- полное
+ создание образа

9. Что из перечисленного НАИМЕНЕЕ подходит для хранения резервных копий?
- жесткий диск
+ оптический диск
- кассета стримера

10. Что из перечисленного НАИБОЛЕЕ подходит для хранения резервных копий?
- жесткий диск
- оптический диск

+ кассета стримера

11. Что из перечисленного НАИБОЛЕЕ подходит для хранения резервных копий?
- флешка
+ жесткий диск
- оптический диск

12. Какой способ резервного копирования осуществляется в режиме реального времени?
- виртуальное
- реальное
- холодное
+ горячее

13. Что необходимо предпринимать для ПОВЫШЕНИЯ надежности резервного копирования?
+ создавать минимум две резервные копии
+ периодически проверять резервные копии
- хранить все копии в одном месте
- доверять резервное копирование самим пользователям

14. Что из перечисленного НЕ ОТНОСИТСЯ к схемам ротации резервных копий?
- одноразовое копирование
- «дед, отец, сын»
+ «Вавилонская башня»
+ инкрементальное копирование

15. Какая из предложенных схем ротации резервных копий самая простая?
+ одноразовое копирование
- простая ротация
- «дед, отец, сын»

16. Какой набор для инкрементального копирования называется «сыном» в схеме ротации «дед, отец, сын»?
+ ежедневное
- еженедельное
- ежемесячное

17. Какой тип RAID дополнительно сохраняет контрольные суммы информации?
- RAID 0
- RAID 1
+ RAID 5
- RAID 10
- JBOD

18. Какой тип RAID предназначен только для повышения производительности и не обладает избыточностью?
+ RAID 0
- RAID 1

- RAID 5
- RAID 10
- JBOD

19. Какой тип RAID состоит из 2-х дисков и информация полностью дублируется на втором диске?
- RAID 0
+ RAID 1
- RAID 5
- RAID 10
- JBOD

20. Какой тип RAID предназначен и для повышения производительности и для повышения сохранности данных?
- RAID 0
- RAID 1
- RAID 5
+ RAID 10
- JBOD

3.Таблица форм тестовых заданий

Всего ТЗ	Из них количество ТЗ в форме			
	закрытых	открытых	на соответствие	на порядок
	шт. %	шт. %	шт. %	шт. %
100%	100	-	-	-

4. Таблица ответов к тестовым заданиям

Верные ответы отмечены знаком « + », неверные отмечены знаком « - ».

Комплект оценочных заданий №8 по Разделу 5. Комплексное обеспечение информационной безопасности, Теме 5.1. Защита информации в персональных компьютерах и Теме 5.2. Защита информации в компьютерных сетях (Аудиторная самостоятельная работа).

1. Спецификация Банка тестовых заданий по Разделу 5. Комплексное обеспечение информационной безопасности, Теме 5.1. Защита информации в персональных компьютерах и Теме 5.2. Защита информации в компьютерных сетях.

2. Содержание Банка тестовых заданий

Инструкция: выбери правильный(е) ответ(ы).

1. Какое из перечисленных средств предназначено для предотвращения кражи ноутбука в общественных местах?
- Датчик движения
- Сканер отпечатков пальцев
+ Замок Кенсингтона

2. Какой тип учетной записи наиболее безопасен для повседневной работы за компьютером?
- Администратора компьютера

- Гость
+ Ограниченная учетная запись

3. Какие из перечисленных устройств могут содержать ВСТРОЕННЫЙ сканер отпечатков пальцев?
+ Ноутбук
+ USB-флешка
+ Внешний жесткий диск
+ Смарфон
- Монитор

4. Какие из перечисленных средств предназначены для защиты от несанкционированного доступа?
- Замок Кенсингтона
+ Mobile Rack
+ Сканер отпечатков пальцев
+ Хранитель экрана (экранная заставка)

5. Какие средства компьютера позволяют установить пароль на вход?
- Сканер отпечатков пальцев
+ Утилита BIOS Setup
+ Учетная запись пользователя
+ Хранитель экрана (экранная заставка)

6. Упаковка передаваемой порции данных, вместе со служебными полями, в новый «конверт», называется – …
- Экранирование
+ Туннелирование
- Архивация

7. Технология, позволяющая обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети, называется – …
- Экранирование
- Туннелирование
+ Виртуальная частная сеть

8. Какой аббревиатурой обозначается понятие «Виртуальная частная сеть»?
- NAS
- WPA
+ VPN

9. Компьютерный тест, используемый для определения, кем является пользователь системы: человеком или компьютером, называется – …
- Баннер
- Краш-тест
+ Капча

10. Какие методы ограничения доступа применяются в беспроводных сетях?

- Скрытый IP-адрес
+ Скрытый SSID
+ Фильтрация MAC-адресов

11. Какие методы аутентификации применяются в беспроводных сетях?
+ WPA аутентификация
+ Открытая
+ По MAC-адресу
- Биометрическая

12. Какие методы шифрования применяются в беспроводных сетях?
+ WPA
+ WEP
- MAC
- VPN

13. Какой метод шифрования применяемый в беспроводных сетях наименее криптостоек?
- WPA
+ WEP
- TKIP

14. Wi-Fi-роутер поддерживает методы шифрования WEP, WPA и WPA2, а ноутбук WEP и WPA, удастся ли использовать WPA2 для их соединения?
- Да, так как достаточно чтобы роутер поддерживал данный метод
+ Нет, необходимо чтобы все устройства поддерживали данный метод

15. Какой алгоритм шифрования применяется при WPA2-шифровании в беспроводных сетях?
- RC-4
+ AES
- ГОСТ 28147-89

16. Какой тип компьютерных сетей обеспечивает лучшую защищенность?
- Беспроводные
+ Проводные

17. Что из перечисленного может называться межсетевым экраном?
+ аппаратное средство, осуществляющее контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами
+ программное средство, осуществляющее контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами
- служба в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам

18. Что из перечисленного является синонимом термина «межсетевой экран»?
+ брандмауэр
+ Firewall
- прокси

- антивирус

19. Какова основная задача межсетевых экранов?
- обеспечение доступа с компьютеров локальной сети в Интернет
+ защита компьютерных сетей или отдельных узлов от несанкционированного доступа
- анонимизация доступа к различным ресурсам

20. Какие существуют виды сетевых экранов в зависимости от охвата контролируемых потоков данных?
+ межсетевые (традиционные)
+ персональные
- локальные

21. Какими из перечисленных возможностей обладают межсетевые экраны?
+ фильтрация доступа
+ контроль доступа
+ уведомление о подозрительной деятельности
- обнаружение вредоносных программ

22. Какие ограничения могут возникнуть при использовании межсетевых экранов?
+ блокирование некоторых сетевых служб
+ снижение пропускной способности
- невозможность выхода в сеть Интернет
- невозможность использования сменных носителей информации

23. Какие режимы работы используются в персональных брандмауэрах?
+ интерактивный (обучения)
+ черный список
+ белый список
- секретный список

24. Как называется служба в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам?
- Firewall
+ прокси-сервер
- брандмауэр

25. Каковы основные функции прокси-серверов?
+ обеспечение доступа с компьютеров локальной сети в Интернет
+ защита локальной сети от внешнего доступа
+ анонимизация доступа к различным ресурсам
- фильтрация сетевых пакетов в соответствии с заданными правилами

3.Таблица форм тестовых заданий

Всего ТЗ	Из них количество ТЗ в форме			
	закрытых	открытых	на соответствие	на порядок
	шт. %	шт. %	шт. %	шт. %

100%	100	-	-	-

4. Таблица ответов к тестовым заданиям

Верные ответы отмечены знаком « + », неверные отмечены знаком « - ».

4.2. Задания для промежуточной аттестации

П Е Р Е Ч Е Н Ь

вопросов для подготовки к экзамену по учебной дисциплине
«ОП.13 Основы информационной безопасности»
для обучающихся по специальности 09.02.07
Информационные системы и программирование

1. Основные принципы информационной безопасности: целостность, доступность, конфиденциальность.
2. Понятие уязвимости, угрозы, источника угрозы информационной безопасности, их классификации.
3. Российское законодательство в области информационной безопасности.
4. Ответственность за нарушение законодательства в информационной сфере.
5. Международные стандарты информационной безопасности. «Оранжевая книга». ISO/IEC 15408 «Общие критерии оценки безопасности информационных технологий».
6. Отечественные стандарты информационной безопасности.
7. Понятие политики информационной безопасности организации. Эффективные и неэффективные политики.
8. Управление персоналом.
9. Физическая защита объектов информатизации.
10. Поддержание работоспособности. Реагирование на нарушение режима безопасности. Планирование восстановительных работ.
11. Принципы управления доступом.
12. Дискреционное управление доступом.
13. Мандатное и ролевое управление доступом.
14. Идентификация и аутентификация.
15. Журналирование и аудит.
16. Криптология. Криптография. Криптоанализ.
17. Классификация методов шифрования.
18. Этапы развития криптографии.
19. Симметричные криптосистемы.
20. Асимметричные криптосистемы.
21. ЭЦП.
22. Алгоритмы шифрования. Реализация алгоритмов шифрования.
23. Классификация вредоносных программ. Пути распространения. Вред, наносимый вредоносными программами.
24. Признаки заражения вредоносными программами.
25. Методы защиты от вредоносных программ.
26. Антивирусные программы.
27. Системы хранения данных. RAID-массивы, сетевые хранилища, ленточные библиотеки и т.п.
28. Резервное копирование информации. Методы и средства резервного копирования. Схемы ротации носителей резервных копий.

29. Защита информации в персональных компьютерах.
30. Угрозы информационной безопасности в компьютерных сетях.
31. Защита информации в компьютерных сетях.
32. Межсетевые экраны и прокси-серверы.

ТЕСТИРОВАНИЕ

1. Спецификация Банка тестовых заданий по курсу учебной дисциплины.
2. Содержание Банка тестовых заданий

Инструкция: выбери правильный(е) ответ(ы).

1. Актуальность и непротиворечивость информации, ее защищенность от РАЗРУШЕНИЯ и НЕСАНКЦИОНИРОВАННОГО ИЗМЕНЕНИЯ, называется …

- конфиденциальностью
+ целостностью
- доступностью

2. Возможность ЗА ПРИЕМЛЕМОЕ ВРЕМЯ получить требуемую информационную услугу, называется …

- конфиденциальностью
- целостностью
+ доступностью

3. Защищенность информации от НЕСАНКЦИОНИРОВАННОГО ДОСТУПА к ней, называется …

+ конфиденциальностью
- целостностью
- доступностью

4. Что из перечисленного относится к основным аспектам информационной безопасности?

+ конфиденциальность
- защищенность
+ целостность
+ доступность

5. Под искажением информации понимают …

- утрату свойств конфиденциальности информации
+ любое преднамеренное или случайное изменение информации
- действие, в результате которого информация перестает физически существовать

6. Под утечкой информации понимают …

+ утрату свойств конфиденциальности информации
- любое преднамеренное или случайное изменение информации
- действие, в результате которого информация перестает физически существовать

7. Под блокированием информации понимают …

- любое преднамеренное или случайное изменение информации
- действие, в результате которого информация перестает физически существовать
+ прекращение или затруднение доступа законных пользователей к информации

8. Возможная опасность совершения какого-либо действия против объекта защиты, называется …
+ угрозой
- уязвимостью
- атакой

9. Присущие объекту свойства, приводящие к нарушению безопасности информации, обусловленные недостатками процесса функционирования объекта, называется …
- угрозой
+ уязвимостью
- атакой

10. Какой из перечисленных источников угроз относится к внешним антропогенным?
+ хакеры
- уборщицы
- пользователи
- вирусы

11. Какие из перечисленных источников угроз относятся к внутренним антропогенным?
- хакеры
+ пользователи
+ уборщицы
- вирусы

12. Какой из перечисленных источников угроз относится к внешним техногенным?
- хакеры
- уборщицы
- некачественные компьютеры
+ средства связи
- ураганы

13. Какие из перечисленных источников угроз относится к внутренним техногенным?
- пользователи
+ уязвимости в ПО
+ некачественные компьютеры
- средства связи

14. Какие из перечисленных источников угроз относятся к стихийным?
- хакеры
- пользователи
- уборщицы
+ ураганы
+ пожары

15. Что из перечисленного является несанкционированным доступом к информации?
+ доступ к информации путём повышения своих прав доступа
+ доступ к информации путём фальсификации своих прав доступа

- доступ к информации санкционированный системным администратором

16. К нарушению, какого аспекта информационной безопасности ведет несанкционированный доступ к информации?
+ конфиденциальности
- доступности
- целостности

17. Какие из перечисленных каналов утечки информации относятся к оптическим?
+ подглядывание за изображением на мониторе
+ фотографирование
- подслушивание
- перехват электромагнитных излучений
- прямое копирование

18. Какие из перечисленных каналов утечки информации относятся к материальным?
+ бумажные документы в мусорной корзине
- удаленные файлы
- электронные подслушивающие закладки («жучки»)
- видеосъемка
+ утерянные носители информации

19. Как называется хакерская атака, когда атакуемый сервер не может обработать огромное количество входящих пакетов?
- социальная инженерия
- IP-спуфинг
- переполнение буфера
+ отказ в обслуживании

20. Чем отличается DDoS атака от DoS атаки?
- атака осуществляется группой хакеров
- атака осуществляется на множество серверов одновременно
+ атака осуществляется с множества компьютеров

21. Как называется метод социальной инженерии, при котором жертве по электронной почте отправляется сообщение, подделанное под официальное письмо – от банка или платёжной системы?
- дорожное яблоко
- троянский конь
+ фишинг

22. Как называется метод социальной инженерии, при котором злоумышленник подбрасывает инфицированный носитель информации в месте, где носитель может быть легко найден?
- претекстинг
- троянский конь
+ дорожное яблоко

23. В каких Российских законодательных актах (реально существующих) рассматриваются вопросы информационной безопасности?
- Закон «О защите информации»
+ Закон «Об информации, информационных технологиях и о защите информации»
- Информационный кодекс РФ
+ Уголовный кодекс РФ

24. За какие виды преступлений в области информационной безопасности предусмотрены наказания в Уголовном кодексе РФ?
+ неправомерный доступ к компьютерной информации
+ создание, использование и распространение вредоносных программ
- использование контрафактной продукции
+ нарушение правил эксплуатации ЭВМ

25. За какие виды преступлений в области информационной безопасности в Уголовном кодексе РФ предусмотрено ЛИШЕНИЕ СВОБОДЫ?
+ неправомерный доступ к компьютерной информации
+ создание, использование и распространение вредоносных программ
- использование контрафактной продукции
+ нарушение правил эксплуатации ЭВМ

26. К какому классу относятся стандарты, регламентирующие различные аспекты реализации и использования средств и методов защиты?
- оценочные
+ спецификации

27. Какой из перечисленных стандартов РФ, является наиболее полным на данный момент и называется также «Общие критерии оценки безопасности информационных технологий»?
- ГОСТ Р 50922-96 Защита информации. Основные термины и определения.
- ГОСТ Р 51275-99 Защита информации. Объект информатизации
+ ГОСТ Р ИСО/МЭК 15408 Методы и средства обеспечения безопасности

28. Какие из перечисленных стандартов являются Российскими?
+ ГОСТ Р 50922-96
+ Р 50.1.053-2005
+ ГОСТ Р ИСО/МЭК 15408
- ISO/IEC 27000
- BS 7799-1:2005
- «Оранжевая книга»
- «Красная книга»

29. Как официально называется стандарт, обычно упоминаемый как «Оранжевая книга»?
- Критерии безопасности информационных систем
- Критерии безопасности компьютерных систем
+ Критерии оценки доверенных компьютерных систем
- Критерии оценки информационных систем

30. Выбери верные ответы:
+ Оранжевая книга является прародителем многих национальных стандартов безопасности ИС
+ Оранжевая книга оценивает степень доверия к ИС в зависимости от используемой в ИС модели управления доступом
+ Оранжевая книга разработана в США
- Оранжевая книга является Британским стандартом

31. Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу, относится к …
+ персональным данным
- государственной тайне
- коммерческой тайне
- личным данным

32. Что из перечисленного относится к основным способам нарушения авторских прав?
+ незаконное копирование
+ незаконное распространение
+ плагиат
- копирайт

33. Что из перечисленного относится к техническим методам защиты авторских прав на программные продукты?
+ электронный ключ
+ серийный номер (ключ, код активации)
+ оригинальный (лицензионный) компакт-диск
+ предоставление функционала этих программ, как сервиса (On-Line)
- невозможности полноценного использования программного продукта без соответствующей поддержки со стороны разработчика

34. Исследование возможности дешифрования информации без знания ключей, называется …
+ криптоанализом
- криптологией
- криптостойкостью

35. Процесс извлечения открытого текста из зашифрованного с использованием криптографического ключа, называется …
+ расшифрованием
- криптологией
- дешифрованием

36. Криптографические методы, использующие и для шифрования, и для дешифрования один и тот же ключ, называются …
- методами асимметричного шифрования
+ методами симметричного шифрования

37. При симметричном шифровании сообщение шифруется при помощи …

- двух ключей
+ закрытого ключа
+ одного и того же ключа
- открытого ключа

38. Что из перечисленного относится к методам симметричного шифрования?
+ шифрование гаммированием
+ шифрование заменой
+ шифрование перестановкой
- шифрование с открытым ключом

39. Как еще называется шифрование заменой?
- перестановка
+ подстановка

40. Как называется шифрование заменой, при которой используется несколько алфавитов?
- монофоническое
+ полиалфавитное
- многоконтурное

41. Как называется шифрование заменой, при которой для редко встречающихся символов применяют один алфавит, а для часто встречающихся – несколько?
+ монофоническое
- полиалфавитное
- многоконтурное

42. Шифрование с использованием в качестве гаммы числа Пи, относится к гаммированию с …
+ бесконечной гаммой
- конечной длинной гаммой
- конечной короткой гаммой

43. Криптографические методы, использующие и для шифрования, и для дешифрования два разных ключа, один из которых закрытый, другой открытый, называются …
+ методами асимметричного шифрования
- методами симметричного шифрования

44. При асимметричном шифровании сообщение шифруется при помощи …
- закрытого ключа
- одного и того же ключа
+ открытого ключа

45. Выбери верное понятие электронной подписи (ЭП):
+ ЭП – это реквизит ЭЛЕКТРОННОГО документа, предназначенный для удостоверения источника данных и защиты данного электронного документа от ПОДДЕЛКИ
- ЭП – это реквизит БУМАЖНОГО документа, предназначенный для удостоверения источника данных и защиты данного электронного документа от ПОДДЕЛКИ

- ЭП – это реквизит ЭЛЕКТРОННОГО документа, предназначенный для удостоверения источника данных и защиты данного электронного документа от НЕСАНКЦИОНИРОВАННОГО ИСПОЛЬЗОВАНИЯ

46. Преобразование входного массива данных произвольной длины в выходную битовую строку фиксированной длины, называется …
+ хэшированием
- электронной подписью
- кодированием

47. Электронная подпись (ЭП) обеспечивает:
+ удостоверение источника документа
+ защиту от изменений документа
- защиту от несанкционированного использования
+ невозможность отказа от авторства

48. Для создания ЭП используется …
+ закрытый ключ
- открытый ключ

49. Какие из перечисленных алгоритмов шифрования предназначены для создания хеш-функций?
- DES
+ MD5
+ SHA
- AES

50. Какие из перечисленных алгоритмов относятся к симметричным?
+ DES
- RSA
+ AES
- MD5

51. Какие из перечисленных алгоритмов относятся к асимметричным?
+ RSA
+ DSA
- AES
+ MD5

52. Какие из перечисленных алгоритмов шифрования НЕ МОГУТ использоваться в Российских государственных учреждениях?
- ГОСТ Р 34.10-2001
+ MD5
+ SHA
+ IDEA
+ AES

53. Процесс сообщения субъектом своего имени или номера, с целью отличить данный субъект от других субъектов, называется – …
- авторизацией
- аутентификацией
+ идентификацией

54. Предоставление субъекту некоторых прав и проверка их наличия, называется – …
+ авторизацией
- аутентификацией
- идентификацией

55. Процедура проверки соответствия субъекта и того, за кого он пытается себя выдать, с помощью некой уникальной информации, называется – …
- авторизацией
+ аутентификацией
- идентификацией

56. К какому *виду* аутентификационных сущностей относятся пароли?
- нечто, чем владеет субъект
+ нечто, что знает субъект
- нечто, что является частью субъекта

57. К какому виду аутентификационных сущностей относится USB-ключ?
+ нечто, чем владеет субъект
- нечто, что знает субъект
- нечто, что является частью субъекта

58. К какому виду аутентификационных сущностей относятся отпечатки пальцев?
- нечто, чем владеет субъект
- нечто, что знает субъект
+ нечто, что является частью субъекта

59. Что из перечисленного применяется для повышения надежности парольной аутентификации?
- использование единого пароля для всех сервисов
+ использование одноразовых паролей
+ ограничение числа неудачных попыток ввода
+ периодическая смена паролей

60. Какие из приведенных примеров паролей МОЖНО считать надежными?
+ g1f2h3j4k5m6
- c1$d
- 1234567890
+ y&7h2*sv

61. Какой метод парольной аутентификации более надежен?
+ на основе одноразовых паролей
- на основе многоразовых паролей

62. Что из себя представляет программный продукт Kerberos?
+ сервер аутентификации
- сервер идентификация
- центр авторизации

63. Происходит ли при использовании программного продукта Kerberos передача паролей по сети?
+ нет
- да

64. Лицо или процесс, действие которого регламентируются правилами разграничения доступа, называется …
+ субъектом
- объектом
- клиентом
- пользователем

65. Единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа, называется …
- субъектом
+ объектом
- клиентом
- файлом

66. Как еще называется мандатное управление доступом?
+ принудительное
- произвольное
- ролевое
- избирательное

67. Как еще называется произвольное управление доступом?
- мандатное
+ дискреционное
+ избирательное

68. В какой модели управления доступом применяются списки или матрицы доступа?
- мандатной
+ дискреционной
- ролевой
- любой

69. В какой модели управления доступом применяются метки безопасности (конфиденциальности)?
+ мандатной
- дискреционной
- ролевой
- любой

70. Кто устанавливает права доступа к конкретному объекту в ДИСКРЕЦИОННОЙ модели управления доступом?
- любой пользователь
- только системный администратор
+ владелец объекта
- сама система

71. Кто устанавливает права доступа к конкретному объекту в МАНДАТНОЙ модели управления доступом?
- любой пользователь
- только системный администратор
- владелец объекта
+ сама система

72. Классическая система дискреционного управления доступом, также называемая «закрытой» подразумевает, что изначально …
+ объект не доступен никому, и в списке прав доступа описывается список разрешений
- объект доступен всем, и в списке прав доступа описывается список ограничений
?
73. Какая модель управления доступом обеспечивает наилучшую защиту конфиденциальности?
- дискреционная
+ мандатная
- ролевая
- любая

74. Что из перечисленного понимаете под термином журналирование?
- анализ накопленной информации
- сбор и накопление информации о *событиях*, происходящих в информационной системе
+ процесс записи информации о происходящих с каким-то объектом событиях в журнал

75. Что из перечисленного понимаете под термином аудит?
+ анализ накопленной информации
- сбор и накопление информации о *событиях*, происходящих в информационной системе
- процесс записи информации о происходящих с каким-то объектом событиях в журнал

76. В активном аудите к ошибкам первого рода относится?
+ пропуск атаки
- ложное срабатывание

77. Действия, выполняемые в рамках имеющихся полномочий, но нарушающие политику безопасности, называются – …
- присвоением полномочий
+ злоупотреблением полномочиями
- нарушением полномочий

78. Какие из перечисленных файловых систем относятся к журналируемым?

+ NFS+
+ NTFS
- FAT32
+ ext3fs
- ext2fs

79. Что из перечисленного может называться межсетевым экраном?
+ аппаратное средство, осуществляющее контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами
+ программное средство, осуществляющее контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами
- служба в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам

80. Что из перечисленного является синонимом термина «межсетевой экран»?
+ брандмауэр
+ Firewall
- прокси
- антивирус

81. Какова основная задача межсетевых экранов?
- обеспечение доступа с компьютеров локальной сети в Интернет
+ защита компьютерных сетей или отдельных узлов от несанкционированного доступа
- анонимизация доступа к различным ресурсам

82. Какие существуют виды сетевых экранов в зависимости от охвата контролируемых потоков данных?
+ межсетевые (традиционные)
+ персональные
- локальные

83. Какими из перечисленных возможностей обладают межсетевые экраны?
+ фильтрация доступа
+ контроль доступа
+ уведомление о подозрительной деятельности
- обнаружение вредоносных программ

84. Какие ограничения могут возникнуть при использовании межсетевых экранов?
+ блокирование некоторых сетевых служб
+ снижение пропускной способности
- невозможность выхода в сеть Интернет
- невозможность использования сменных носителей информации

85. Какие режимы работы используются в персональных брандмауэрах?
+ интерактивный (обучения)
+ черный список
+ белый список
- секретный список

86. Как называется служба в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам?
- Firewall
+ прокси-сервер
- брандмауэр

87. Каковы основные функции прокси-серверов?
+ обеспечение доступа с компьютеров локальной сети в Интернет
+ защита локальной сети от внешнего доступа
+ анонимизация доступа к различным ресурсам
- фильтрация сетевых пакетов в соответствии с заданными правилами

88. Что из перечисленного относится к вредоносным программам?
+ Backdoor-утилиты
- Backup-утилиты
+ Сетевые черви
+ Троянские программы

89. Выбери верные варианты ответов:
+ вредоносные программы способны заразить файлы на flash-карте при её чтении
- вредоносные программы способны заразить файлы на оптическом диске при его чтении
+ вредоносные программы способны стереть информацию на жестком диске

90. Как называется программа, распространяющаяся по сетевым каналам, способная к автономному преодолению систем защиты, а также к созданию и дальнейшему распространению своих копий?
- Вирус
+ Сетевой червь
- Троянская программа

91. Как называется программа, способная создавать свои копии и внедрять их в файлы, системные области компьютера, а также осуществлять иные деструктивные действия?
+ Вирус
- Сетевой червь
- Троянская программа

92. Как называется программа, отличающаяся отсутствием механизма создания собственных копий и проникающая в компьютер под видом полезных программ?
- Вирус
- Сетевой червь
+ Троянская программа

93. Какие виды вредоносных программ создают свои вирусные копии в зараженном компьютере?
+ Вирусы
+ Сетевые черви
- Троянские программы

94. Какие типы файлов способны заразить файловые вирусы?
+ exe
+ dll
- avi
- doc

95. Какие типы файлов способны заразить макровирусы?
- exe
+ xls
+ doc
- txt

96. Какие типы файлов способны заразить скрипт-вирусы?
- exe
- doc
+ vbs
+ js

97. Вирусы, какого вида постоянно находятся в оперативной памяти компьютера?
+ резидентные
- нерезидентные

98. Какие из перечисленных видов червей бывают?
+ P2P
- Загрузочные
+ Почтовые
+ Сетевые
- Файловые

99. По выполняемым функциям троянские программы бывают:
+ Клавиатурные шпионы
+ Вымогатели
+ Похитители паролей
- Мониторные шпионы
+ Модификаторы настроек браузера

100. Какие способы проникновения в компьютер используют троянские программы?
+ Кооперация
+ Маскировка
- Полиморфизм
- Сканирование портов

101. Что из перечисленного может являться причинами проникновения вредоносных программ в компьютер с установленной антивирусной программой?
+ Антивирус отключен
+ Вирус еще не известен антивирусу
- Используется бесплатный антивирус

+ Устаревшие антивирусные базы

102. Где следует искать проявления присутствия вирусов в системе?
+ диспетчер задач
- панель управления
+ системный реестр
+ автозагрузка

103. Что из перечисленного относится к организационным методам защиты от вредоносных программ?
+ Не открывать почтовые сообщения от незнакомых отправителей
+ Проверять на наличие вирусов файлы, загружаемые из сети Интернет
- Использовать брандмауэры
- Устанавливать обновления операционной системы
+ Регулярно обновлять антивирусные базы

104. Что из перечисленного относится к техническим методам защиты от вредоносных программ?
- Не открывать почтовые сообщения от незнакомых отправителей
+ Использовать брандмауэры
- Регулярно обновлять антивирусные базы
+ Устанавливать обновления прикладных программ
+ Устанавливать обновления операционной системы
+ Использовать антиспам-фильтры

105. Технология обнаружения вредоносных программ, основанная на нахождении, уникальная последовательности байт, присутствующей в данном вирусе и не встречающейся в других программах называется – …
+ Сигнатурным анализом
- Вероятностным анализом
- Эмуляционным анализом

106. Какие технологии относятся к так называемой проактивной защите?
+ Поведенческий анализ
- Сигнатурный анализ
+ Песочница
+ Эвристический анализ

107. Что из перечисленного способен произвести антивирус с найденной вредоносной программой, используя СИГНАТУРНЫЕ методы обнаружения?
- Выдать сообщение о наличие подозрительного объекта
+ Отправить файл в карантин
+ Попытаться вылечить файл
+ Удалить инфицированный файл

108. Что из перечисленного способен произвести антивирус с найденной вредоносной программой, используя ВЕРОЯТНОСТНЫЕ методы обнаружения?
+ Выдать сообщение о наличие подозрительного объекта

- Отправить файл в карантин
- Попытаться вылечить файл
- Удалить инфицированный файл

109. Что входит в минимальный набор возможностей обычного антивируса?
- Брандмауэр
+ Модуль обновления антивирусной базы
+ Монитор
+ Сканер
- Проактивная защита

110. Какой модуль антивирусной программы проверяет все файлы и процессы, находящиеся в оперативной памяти?
- Модуль обновления антивирусной базы
+ Монитор
- Сканер
- Брандмауэр

111. Какой модуль антивирусной программы проводит полную проверку файлов хранящихся на всех носителях информации?
- Антихакер
- Монитор
+ Сканер
- Брандмауэр

112. Чем отличается облачный антивирус от обычного?
- Не умеет лечить зараженные файлы
+ Не требуется обновлять антивирусные базы
+ Функционирует только при наличии подключения к сети Интернет
+ Антивирусная база находится в Интернете

113. Каким еще термином обозначается резервное копирование?
+ Backup
- Background
- Backdoor

114. При каком виде резервного копирования создается первая копия полная, вторая – отличие от первой, третья снова полная и т.д.?
+ дифференциальном
- инкрементальном
- интегральном

115. При каком виде резервного копирования создается первая копия полная, вторая – отличие от первой, третья – отличие от второй и т.д.?
- дифференциальном
+ инкрементальном
- интегральном

116. Какой вид резервного копирования занимает БОЛЬШЕ всего места на носителях информации?
- дифференциальный
+ полный
- инкрементальный

117. Какой вид резервного копирования самый ЭКОНОМНЫЙ с точки зрения занимаемого места на носителях информации?
- дифференциальный
- полный
+ инкрементальный

118. Как называется вид резервного копирования, при котором создается своеобразный «снимок» жесткого диска и копируется на носитель сектор за сектором?
- клонирование
- полное
+ создание образа

119. Что из перечисленного НАИБОЛЕЕ подходит для хранения резервных копий?
- жесткий диск
- оптический диск
+ лента (кассета) стримера

120. Что из перечисленного НАИБОЛЕЕ подходит для хранения резервных копий?
- флешка
+ жесткий диск
- оптический диск

121. Какой способ резервного копирования осуществляется в режиме реального времени?
- виртуальное
- реальное
- холодное
+ горячее

122. Что из перечисленного НЕ ОТНОСИТСЯ к схемам ротации резервных копий?
- одноразовое копирование
- «дед, отец, сын»
+ «Вавилонская башня»
+ инкрементальное копирование

123. Какой тип RAID дополнительно сохраняет контрольные суммы информации?
- RAID 0
- RAID 1
+ RAID 5
- RAID 10

124. Какой тип RAID предназначен только для повышения производительности и не обладает избыточностью?

+ RAID 0
- RAID 1
- RAID 5
- RAID 10

125. Какой тип RAID состоит из 2-х дисков и информация полностью дублируется на втором диске?
- RAID 0
+ RAID 1
- RAID 5
- RAID 10

126. Какой тип RAID предназначен и для повышения производительности и для повышения сохранности данных?
- RAID 0
- RAID 1
- RAID 5
+ RAID 10

127. Какое из перечисленных средств предназначено для предотвращения кражи ноутбука в общественных местах?
- Датчик движения
- Сканер отпечатков пальцев
+ Замок Кенсингтона

128. Какой тип учетной записи наиболее безопасен для повседневной работы за компьютером?
- Администратора компьютера
- Гость
+ Ограниченная учетная запись

129. Какие из перечисленных устройств могут содержать ВСТРОЕННЫЙ сканер отпечатков пальцев?
+ Ноутбук
+ USB-флешка
+ Внешний жесткий диск
+ Смарфон
- Монитор

130. Какие средства компьютера позволяют установить пароль на вход?
- Сканер отпечатков пальцев
+ Утилита BIOS Setup
+ Учетная запись пользователя
+ Хранитель экрана (экранная заставка)

131. Упаковка передаваемой порции данных, вместе со служебными полями, в новый «конверт», называется – …
- Экранирование

+ Туннелирование
- Архивация

132. Технология, позволяющая обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети, называется – …
- Экранирование
- Туннелирование
+ Виртуальная частная сеть

133. Какой аббревиатурой обозначается понятие «Виртуальная частная сеть»?
- NAS
- WPA
+ VPN

134. Компьютерный тест, используемый для определения, кем является пользователь системы: человеком или компьютером, называется – …
- Баннер
- Краш-тест
+ Капча

135. Какие методы ограничения доступа применяются в беспроводных сетях?
- Скрытый IP-адрес
+ Скрытый SSID
+ Фильтрация MAC-адресов

136. Какие методы аутентификации применяются в беспроводных сетях?
+ WPA аутентификация
+ Открытая
+ По MAC-адресу
- Биометрическая

137. Какие методы шифрования применяются в беспроводных сетях?
+ WPA
+ WEP
- MAC
- VPN

138. Какой метод шифрования применяемый в беспроводных сетях наименее криптостоек?
- WPA
+ WEP
- TKIP

139. Какой тип компьютерных сетей обеспечивает лучшую защищенность?
- Беспроводные
+ Проводные

140. В каком месте организации должна находиться серверная комната с точки зрения информационной безопасности?
+ вдали от основного потока посетителей
- точно в географическом центре организации
- ближе к главному входу в здание
- ближе к кабинету руководителя организации

141. Что из перечисленного можно использовать в качестве электронных систем обнаружения злоумышленников?
+ охранную сигнализацию
- кодовые замки
+ камеры видеонаблюдения
- межсетевые экраны

142. Какой тип замка может позволять устанавливать различные комбинации для каждого пользователя и вести журнал событий регистрации пользователей?
+ электронный
- механический
- любой кодовый

143. Какие типы датчиков используются для физической защиты серверной комнаты?
+ пожарные
+ охранные
+ протечки воды
- обрыва кабеля питания

144. Что из перечисленного относится к охранной сигнализации?
+ емкостные датчики
+ датчики движения
+ инфракрасные (лазерные) датчики
+ вибрационные датчики
- дымовые датчики

145. Что из перечисленного относится к пожарной сигнализации?
- емкостные датчики
+ тепловые датчики
- датчики протечки
- вибрационные датчики
+ дымовые датчики

146. Что представляет собой комната ИТ-безопасности?
+ модульная конструкция типа помещение в помещении
- кабинет обучения информационной безопасности
- помещение, в котором обеспечена защита от прослушивания

147. К уровню обеспечения информационной безопасности предприятия относится Политика информационной безопасности?
+ административный

- программно-технический
- нормативно-правовой

148. Что из перечисленного можно считать эффективной Политикой информационной безопасности предприятия?
+ совокупность нормативных документов, инструкций, регламентов, процедур и т.п. в области информационной безопасности
- комплект инструкций для пользователей в области информационной безопасности
- пакет документов на тему информационной безопасности

149. Каким способом лучше создавать эффективную Политику информационной безопасности?
+ разработать самостоятельно
- взять готовую в сети Интернет
- использовать соответствующий ГОСТ

150. Как называется раздел Политики информационной безопасности, подтверждающий заинтересованность высшего руководства организации проблемами информационной безопасности?
+ вводный раздел
- раздел управления
- юридический раздел
- раздел физической защиты

151. Как называется раздел Политики информационной безопасности, описывающий подход к управлению компьютерами и сетями передачи данных?
- вводный раздел
+ раздел управления
- юридический раздел
- раздел физической защиты

152. Как называется раздел Политики информационной безопасности, подтверждающий соответствие политики информационной безопасности текущему законодательству?
- вводный раздел
- раздел управления
+ юридический раздел
- раздел физической защиты

153. В каком разделе Политики информационной безопасности могут быть описаны типы помещений организации и необходимые для них меры безопасности?
- вводный раздел
- раздел управления
- юридический раздел
+ раздел физической защиты

154. Выделение пользователям только тех прав доступа, которые необходимы им для выполнения служебных обязанностей, называется – …
+ минимизацией привилегий

- разделением обязанностей
- минимизацией обязанностей
- разделением привилегий

155. Распределение ролей и ответственности, так чтобы один человек не мог нарушить критически важный для организации процесс, называется – …
- минимизацией привилегий
+ разделением обязанностей
- минимизацией обязанностей
- разделением привилегий

156. В каких случаях необходимо ликвидировать права доступа пользователя?
+ при увольнении сотрудника
- при нахождении сотрудника в отпуске
+ при смене должности сотрудником
- при получении выговора сотрудником

3. Таблица форм тестовых заданий

Всего ТЗ	Из них количество ТЗ в форме			
	закрытых	открытых	на соответствие	на порядок
	шт. %	шт. %	шт. %	шт. %
100%	100%	0%	0%	0%

4. Таблица ответов к тестовым заданиям

Верные ответы отмечены знаком « + », неверные отмечены знаком « - ».