МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«АРКТИЧЕСКИЙ ГОСУДАРСТВЕННЫЙ АГРОТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО Арктический ГАТУ)
Колледж технологий и управления

Регистрационный № 24-1/34

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Дисциплина **ОП.13 Информационная безопасность**

Специальность **09.02.07. Информационные системы и программирование**

Квалификация **Программист**

Уровень ППССЗ **базовая**

Срок освоения ППССЗ **3 г 10 мес**

Форма обучения **очная**

Общая трудоемкость **32 ч**

Якутск 2024

Рабочая программа учебной дисциплины разработана в соответствии с:

- Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 09.02.07 Информационные системы и программирование, утвержденный приказом Министерства образования и науки Российской Федерации от 09 декабря 2016 г. №1547.
- Учебным планом специальности 09.02.07 Информационные системы и программирование, одобрен Ученым советом ФГБОУ ВО Арктический ГАТУ № 24 от 30.05.2024 г.

Разработчик(и) РПД Попова Вилена Гаврильевна – преподаватель

Председатель ЦК ГиЕД _____ /Васильева Е.К./
подпись фамилия, имя, отчество

Протокол заседания ЦК ГиЕД № 10 от « 24 » мая 2024 г.

Директор КТиУ _____ /Яковлева Н.М./
подпись фамилия, имя, отчество

« 24 » мая 2024 г

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ
ОП.13 Информационная безопасность

1.1. Область применения программы

Рабочая программа учебной дисциплины является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности (специальностям) СПО 09.02.07 Информационные системы и программирование.

1.2. Место учебной дисциплины в структуре программы подготовки специалистов среднего звена:

Учебная дисциплина «Информационная безопасность» относится к общепрофессиональному циклу.

Освоение дисциплины способствует формированию компетенций:

ОК 01. Выбирать способы решения задач в профессиональной деятельности, применительно к различным контекстам;

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности;

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами;

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста;

ОК 09. Использовать информационные технологии профессиональной деятельности;

ОК 10. Пользоваться профессиональной на государственном и иностранном языке.

1.3. Цели и задачи учебной дисциплины – требования к результатам освоения учебной дисциплины:

Программа ориентирована на достижение следующих целей:

•усвоение знаний по нормативно-правовым основам организации информационной безопасности, изучение стандартов и руководящих документов по защите информационных систем;

•ознакомление с основными угрозами информационной безопасности;

•правилами их выявления, анализа и определение требований к различным уровням обеспечения информационной безопасности;

•формирование научного мировоззрения, навыков индивидуальной самостоятельной работы с учебным материалом.

Содержание каждой темы включает теоретический и практико- ориентированный материал, реализуемый в форме лабораторной работы с использованием средств ИКТ.

В результате освоения учебной дисциплины обучающийся должен уметь:

- У.1 классифицировать компьютерные вирусы.
- У.2 определять вирусоподобные программы по характерным признакам
- У.3 классифицировать антивирусные программы
- У.4 использовать механизмы идентификации и аутентификации для защиты информационных систем.

В результате освоения учебной дисциплины обучающийся должен знать:

- З.1 характерные черты компьютерных вирусов;
- З.2 проблемы при определении компьютерного вируса.
- З.3 классы компьютерных вирусов;
- З.4 характеристику различных компьютерных вирусов.
- З.5 принципы защиты распределенных вычислительных сетей

1.4. Рекомендуемое количество часов на освоение программы учебной дисциплины:

Максимальной учебной нагрузки обучающегося 32 часа, в том числе:
- обязательной аудиторной учебной нагрузки обучающегося 32 часа.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем часов**
Максимальная учебная нагрузка (всего)	32
Обязательная аудиторная учебная нагрузка (всего)	32
в том числе:	
лекции	16
практические занятия	16
Итоговая аттестация в форме зачета в пятом семестре	

2.2. Тематический план и содержание учебной дисциплины Информационная безопасность

Наименование разделов и тем	*Содержание учебного материала и формы организации деятельности обучающихся*	*Объем в часах*	*Уровень освоения*
	Раздел 1. Информационная безопасность и уровни ее обеспечения	***6***	
Тема 1. Понятие "информационная безопасность"	***Содержание учебного материала***	6	1,2
	.Понятие "информационная безопасность". Задачи информационной безопасности, уровни формирования режима информационной безопасности. Нормативно-правовые основы информационной безопасности. Стандарты информационной безопасности в РФ. Классификация угроз "информационной безопасности".		
	В том числе практических занятий	2	1,2,3
	Раздел 2. Компьютерные вирусы и защита от них.	8	
Тема 2.Вирусы как угроза информационной безопасности	***Содержание учебного материала***	8	1,2
	Вирусы как угроза информационной безопасности. Классификация компьютерных вирусов. Характеристика "вирусоподобных" программ. Антивирусные программы. Профилактика компьютерных вирусов. Обнаружение неизвестного вируса.		
	В том числе практических занятий	6	1,2,3
	Раздел 3. Информационная безопасность вычислительных сетей		

Тема 3. Особенности обеспечения информационной безопасности в компьютерных сетях.	***Содержание учебного материала***	8	
	Особенности обеспечения информационной безопасности в компьютерных сетях. Сетевые модели передачи данных. Модель взаимодействия открытых систем OSI/ISO. Адресация в глобальных сетях. Классификация удаленных угроз в вычислительных сетях. Типовые удаленные атаки и их характеристика. Причины успешной реализации удаленных угроз в вычислительных сетях. Принципы защиты распределенных вычислительных сетей	8	1,2
	В том числе практических занятий	4	1,2,3
	Раздел 4. Механизмы обеспечения "информационной безопасности"	8	
Тема 4. Идентификация и аутентификация.	***Содержание учебного материала***	8	
	Тема 4. Идентификация и аутентификация. Криптография и шифрование. Методы разграничение доступа. Регистрация и аудит. Межсетевое экранирование. Технология виртуальных частных сетей (VPN) составляющие технологии виртуальных частных сетей.		1,2
	В том числе практических занятий	4	1,2,3
Примерный перечень практических работ: 1. распределять задачи информационной безопасности по уровням ее обеспечения 2. определять политику безопасности организации, Конституция Российской Федерации, доктрина информационной безопасности Российской Федерации, федеральные законы в области информации и информационной безопасности, указы президента РФ и постановления правительства РФ в области информации и информационной безопасности, правовые режимы защиты информации. 3. выявлять и классифицировать угрозы информационной безопасности 4. проводить профилактику компьютерных вирусов. 5. проверить систему на наличие макровируса 6. использовать модель OSI/ISO для описания процесса передачи данных между узлами компьютерной сети. 7. преобразовывать двоичный IP-адрес в десятичный, определять тип сети по IP-адресу. 8. классифицировать типовые удаленные атаки по совокупности признаков. 9. использовать электронную цифровую подпись для проверки целостности данных. 10. использовать механизмы регистрации и аудита для анализа защищенности системы.			
Всего:		*32*	

3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечения

№ п\п	Наименование дисциплины (модуля), практик в соответствии с учебным планом	Наименование специальных* помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
1	ОП.13 Информационная безопасность	**Лаборатория информационных ресурсов** 677007, Республика Саха (Якутия), г. Якутск, ш. Сергеляхское, 3 км, д.3, 4 этаж, №14	**Оборудование:** Автоматизированные рабочие места на 15 обучающихся (обучающихся с конфигурацией: Core i5 дискретная видеокарта, 8GB ОЗУ, один или два монитора 23", 24”ViewsonicVA2407h, мышь, клавиатура; Автоматизированное рабочее место преподавателя (Rusco Core-i5-7100/2*4Gb/500Gb/Win10Pro/Office, монитор (22”Benq GL2250) – 1; **Учебная мебель:** компьютерный стол (СК № 20164 (КР - груша, Д - 024)) – 22 шт.; стул подъемно-поворотный – 16 шт Офисный мольберт (флипчарт); Проектор и экран; Маркерная доска; Принтер А3, цветной; МФУ формата А4; **Программное обеспечение общего и профессионального назначения**

3.2. Информационное обеспечение обучения

Перечень учебных изданий, интернет-ресурсов, дополнительной литературы

Основные источники:

№	Наименование	Авторы	Год и место издания	Используется при изучении тем	Семестр
1	2	3	4	5	6
1	Основы информационной безопасности: надежность и безопасность программного обеспечения: учебное пособие для среднего профессионального образования / — 342 с Режим доступа: https://www.biblio-online.ru/viewer/osnovy-informacionnoy-bezopasnosti-nadezhnost-i-bezopasnost-programmnogo-obespecheniya-456792#page/1	О. В. Казарин, И. Б. Шубинский.	Москва: Издательство Юрайт, 2020	1-4	5

Перечень электронных ресурсов:

№	Наименование
Э1	www.fcior.edu.ru (Федеральный центр информационно-образовательных ресурсов — ФЦИОР).
Э2	www. school-collection.edu.ru (Единая коллекция цифровых образовательных ресурсов).
Э3	www. intuit. ru/studies/courses (Открытые интернет-курсы «Интуит» по курсу «Информатика»)
Э4	www. lms. iite. unesco. org (Открытые электронные курсы «ИИТО ЮНЕСКО» по информационным технологиям).
Э5	http://ru.iite.unesco.org/publications (Открытая электронная библиотека «ИИТО ЮНЕСКО» по ИКТ в образовании).
Э6	www.megabook.ru (Мегаэнциклопедия Кирилла и Мефодия, разделы «Наука / Математика. Кибернетика» и «Техника / Компьютеры и Интернет»).
Э7	www.ict. edu. ru (портал «Информационно-коммуникационные технологии в образовании»).
Э8	www.digital-edu.ru (Справочник образовательных ресурсов «Портал цифрового образования»)
Э9	www.window. edu. ru (Единое окно доступа к образовательным ресурсам Российской Федерации)
Э10	www. freeschool.altlinux.ru (портал Свободного программного обеспечения
Э11	www.heap.altlinux.org/issues/textbooks (учебники и пособия по Linux)
Э12	www.books.altlinux. ru/altlibrary/openoffice (электронная книга «OpenOffice. org: Теория и практика»)
Э1	Учебники по программированию http://programm.ws/index.php

Перечень информационных справочных систем:

№	Наименование
1	Информационно-правовая система Гарант

3.3. Условия реализации учебной дисциплины для студентов-инвалидов и лиц с ограниченными возможностями здоровья

3.3.1. Образовательные технологии.

С целью оказания помощи в обучении студентов-инвалидов и лиц с ОВЗ применяются образовательные технологии с использованием универсальных, специальных информационных и коммуникационных средств.

Для основных видов учебной работы применяются:

Контактная работа:

- лекции – проблемная лекция, лекция-дискуссия, лекция-диалог, лекция-консультация, лекция с применением дистанционных технологий и привлечением возможностей Интернета;
- практические (семинарские) занятия - практические задания;
- групповые консультации – опрос, работа с лекционным и дополнительным материалом;
- индивидуальная работа с преподавателем - индивидуальная консультация, работа с лекционным и дополнительным материалом, беседа, морально-эмоциональная поддержка и стимулирование, дистанционные технологии.

Формы самостоятельной работы устанавливаются с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге или на компьютере).

В качестве самостоятельной подготовки в обучении используется - система дистанционного обучения Moodle (sdo.agatu.ru).

Самостоятельная работа:

- работа с книгой и другими источниками информации, план-конспекты;
- творческие самостоятельные работы;
- дистанционные технологии.

При необходимости обучающимся предоставляется дополнительное время для консультаций и выполнения заданий.

3.3.2. Специальное материально-техническое и учебно-методическое обеспечение.

При обучении по дисциплине используется система, поддерживающая дистанционное образование - «Moodle» (sdo.agatu.ru), ориентированная на организацию дистанционных курсов, а также на организацию взаимодействия между преподавателем и обучающимися посредством интерактивных обучающих элементов курса.

Для обучающихся лиц с нарушением зрения предоставляются:

- видеоувеличитель-монокуляр для просмотра Levenhuk Wise 8x25;
- электронный ручной видеоувеличитель видео оптик “wu-tv”;
- возможно также использование собственных увеличивающих устройств;
- версия сайта академии http://www.agatu.ru/ для слабовидящих.

Для обучающихся лиц с нарушением слуха предоставляются:

- аудитории со звукоусиливающей аппаратурой (колонки, микрофон);
- компьютерная техника в оборудованных классах;
- учебные аудитории с мультимедийной системой с проектором;
- аудитории с интерактивными досками в аудиториях;
- учебные пособия, методические указания в форме электронного документа

Для обучающихся лиц с нарушениями опорно-двигательного аппарата предоставляются:

- система дистанционного обучения Moodle (sdo.agatu.ru);
- учебные пособия, методические указания в форме электронного документа/

3.3.3. Контроль и оценка результатов освоения учебной дисциплины.

Контроль результатов обучения осуществляется в процессе проведения практических занятий, выполнения индивидуальных самостоятельных работ.

Формы и сроки проведения рубежного контроля определяются с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.), и может проводиться в несколько этапов.

При необходимости, предоставляется дополнительное время для подготовки ответов на зачете, аттестация проводится в несколько этапов (по частям), во время аттестации может присутствовать ассистент, аттестация прерывается для приема пищи, лекарств, во время аттестации используются специальные технические средства.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения практических занятий и лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Итоговый контроль:	Зачет
Уметь	
У.1 классифицировать компьютерные вирусы	•Тестирование. •Контрольная работа •Самостоятельная работа. •Наблюдение за выполнением практического задания. (деятельностью студента) •Оценка выполнения практического задания(работы)
У.2 определять вирусоподобные программы по характерным признакам	
У.3 классифицировать антивирусные программы	
У.4использовать механизмы идентификации и аутентификации для защиты информационных систем	
Знать	
З.1 характерные черты компьютерных вирусов	
З.2 проблемы при определении компьютерного вируса	
З.3 классы компьютерных вирусов	
З.4 характеристику различных компьютерных вирусов	
З.5 принципы защиты распределенных вычислительных сетей	

Лист изменений и дополнений общих компетенций
по специальности
09.02.07 Информационные системы и программирование

Актуализированы новые общие компетенции приказ Минпросвещения России от 03.07.2024 №464 по специальности 09.02.07 Информационные системы и программирование:

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях; (в ред. Приказа Минпросвещения России от 03.07.2024 N 464);

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения; (в ред. Приказа Минпросвещения России от 03.07.2024 N 464);

ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках. (п. 3.2 в ред. Приказа Минпросвещения России от 01.09.2022 N 796).

Председатель МК КТиУ Ваганова В.Г.

Протокол заседания МК КТиУ от «06» сентября 2024 г. № 1.

МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Арктический государственный агротехнологический университет»
Колледж технологий и управления

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по учебной дисциплине

ОП.13 Информационная безопасность

09.02.07. Информационные системы и программирование

Якутск 2024 г.

Фонд оценочных средств учебной дисциплины разработан в соответствии с:

- Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 09.02.07. Информационные системы и программирование, утвержденный приказом Министерства образования и науки Российской Федерации от 09 декабря 2016 г. №1547.
- Учебным планом специальности 09.02.07. Информационные системы и программирование одобрен Ученым советом ФГБОУ ВО Арктический ГАТУ Протокол №24 от 30.05.2024г.

Разработчик(и) ФОС Попова Вилена Гаврильевна– преподаватель

Фонд оценочных средств учебной дисциплины ОП 13. Информационная безопасность одобрен на цикловой комиссии гуманитарных и естественных дисциплин от «21» мая 2024 г. Протокол № 10

Председатель ЦК ГиЕД _____ _____ /Васильева Е.К./
подпись фамилия, имя, отчество

Фонд оценочных средств учебной дисциплины рассмотрен и рекомендован к использованию в учебном процессе на заседании методической комиссии Колледжа технологий и управления по специальности 09.02.07. Информационные системы и программирование.

Председатель методической комиссии КТиУ _____ /Сивцева Е.И./
подпись фамилия, имя, отчество

ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

ОП.13 Информационная безопасность
09.02.07 Информационные системы и программирование

Таблица 1

Результаты обучения (освоенные умения, усвоенные знания)[1]	**Формируемые компетенции[1]**	**Наименование темы[2]**	**Уровень освоения Темы[2]**	**Наименование контрольно-оценочного средства**	
				Текущий контроль[3]	**Промежуточная аттестация[4]**
1	2	3	4	5	6
Уметь: - У.1 классифицировать компьютерные вирусы. - У.2 определять вирусоподобные программы по характерным признакам - У.3 классифицировать антивирусные программы -У.4 использовать механизмы идентификации и аутентификации для защиты информационных систем. **Знать**: -З.1 характерные черты компьютерных вирусов; -З.2 проблемы при определении компьютерного вируса. -З.3 классы компьютерных вирусов; -З.4 характеристику различных компьютерных вирусов. -З.5 принципы	**ОК 01.** Выбирать способы решения задач в профессиональной деятельности, применительно к различным контекстам; **ОК 02.** Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности; **ОК 04.** Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами; **ОК 05.** Осуществлять устную и письменную коммуникацию	Тема 1. Понятие "информационная безопасность" Тема 2.Вирусы как угроза информационной безопасности Тема 3. Особенности обеспечения информационной безопасности в компьютерных сетях. Тема 4. Идентификация и аутентификация	1,2	вопросы к устному опросу, контрольные вопросы для защиты практической работы	зачет

защиты распределенных вычислительных сетей	на государственном языке с учетом особенностей социального и культурного контекста; **ОК 09**. Использовать информационные технологии профессиональной деятельности; **ОК 10.** Пользоваться профессиональной на государственном и иностранном языке;				

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ, ПОДЛЕЖАЩИЕ ПРОВЕРКЕ

В результате аттестации по учебной дисциплине осуществляется комплексная проверка следующих умений и знаний, а также динамика формирования общий компетенций.

Таблица 2

Компетенции	Результаты обучения	Основные показатели оценки результата	Формы и методы контроля и оценки
	Знает:		
ОК 01. Выбирать способы решения задач в профессиональной деятельности, применительно к различным контекстам; ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач	-З.1 характерные черты компьютерных вирусов;	Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; Применять основные правила и документы системы сертификации Российской федерации; Классифицировать основные угрозы безопасности информации.	Фронтальный опрос Тестирование Текущий контроль Оценка выполнения практических работ Текущий контроль Промежуточная аттестация в форме: зачет
	-З.2 проблемы при определении компьютерного вируса.		
	-З.3 классы компьютерных вирусов;		
	-З.4 характеристику различных компьютерных вирусов.		

профессиональной деятельности; ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами; ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста; ОК 09. Использовать информационные технологии профессиональной деятельности; ОК 10. Пользоваться профессиональной на государственном и иностранном языке;	-З.5 принципы защиты распределенных вычислительных сетей **Умеет:** - У.1 классифицировать компьютерные вирусы. - У.2 определять вирусоподобные программы по характерным признакам - У.3 классифицировать антивирусные программы -У.4 использовать механизмы идентификации и аутентификации для защиты информационных систем.		

2.1. Оценка освоения учебной дисциплины

2.1.1. Формы и методы оценивания

Предметом оценки служат умения и знания, предусмотренные ФГОС по дисциплине ОП.13 Информационная безопасность направленные на формирование общих компетенций.

Таблица 3

Перечень объектов контроля и оценки

Результаты обучения	Основные показатели оценки результата	Оценка (да/нет)
Знает:		
-З.1 характерные черты компьютерных вирусов;	Сущность и понятие информационной безопасности, характеристику ее составляющих;	да
-З.2 проблемы при определении компьютерного вируса.	Место информационной безопасности в системе национальной безопасности страны;	да
-З.3 классы компьютерных вирусов;	Современные средства и способы обеспечения информационной безопасности.	
-З.4 характеристику различных компьютерных вирусов.	Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;	да
-З.5 принципы защиты распределенных вычислительных сетей	Применять основные правила и документы системы сертификации Российской федерации;	да
Умеет:		
- У.1 классифицировать компьютерные вирусы.	Классифицировать основные угрозы безопасности информации.	да
- У.2 определять вирусоподобные программы по характерным признакам	Место информационной безопасности в системе национальной безопасности страны;	да
- У.3 классифицировать антивирусные программы	Современные средства и способы обеспечения информационной безопасности.	да
-У.4 использовать механизмы идентификации и аутентификации для защиты информационных систем.	Место информационной безопасности в системе национальной безопасности страны;	да

Критерии оценивания:
Оценка компетенции производится по интегральной оценке ОПОР. Каждый ОПОР оценивается 1 или 0, сумма этих оценок дает оценку компетенции: «да» или «нет». Уровень оценки компетенций производится суммированием количества ответов «да» в процентном соотношении от общего количества ответов.
Для перевода баллов в оценку применяется универсальная шкала оценки образовательных достижений

Таблица 3

Универсальная шкала оценки образовательных достижений

Процент результативности	**Оценка уровня подготовки**	
	оценка компетенций обучающихся	**оценка уровня освоения дисциплин;**
90 ÷ 100	высокий	*отлично*
70 ÷ 89	продвинутый	*хорошо*
50 ÷ 69	пороговый	*удовлетворительно*
менее 50	не освоены	*неудовлетворительно*

2.2. **Матрица оценок образовательных достижений обучающихся**

Оценка достижений обучающихся по результатам Зачета учебной дисциплины

ОП.13 Информационная безопасность

Группа ИСиП

Ф.И.О. обучающихся	*Компетенции ОК 1*							*ОК 2*	*ОК 4*	*ОК 5*	*ОК 9*	*ОК 10*				*max балл*	*% выполнения*	*Оценка компетенции****
*Умения и знания**	*У1*	*У2*	*У3*	*У4*	*З1*	*З2*	*З3*	*З4*	*З5*									
*Величина баллов **	*10*	*5*	*5*	*5*	*5*	*5*	*5*	*5*	*5*							*50*	*100 %*	*отлично*

*- *включаете все умения и знания, которые указаны в ФГОС СПО специальности*

**- *величину баллов за одно умение и знание определяете самостоятельно. Сумму баллов пересчитываете в проценты.*

***- *при оценке компетенций необходимо воспользоваться «Универсальной шкалой оценки»:*

90 – 100 %	*высокий*	*отлично*
70 – 89 %	*продвинутый*	*хорошо*
50 – 69 %	*пороговый*	*удовлетворительно*
менее 50 %	*не освоены*	*неудовлетворительно*

МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«АРКТИЧЕСКИЙ ГОСУДАРСТВЕННЫЙ АГРОТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО Арктический ГАТУ)
Колледж технологий и управления

Комплект
контрольно-измерительных материалов
для текущего контроля

ОП.13 Информационная безопасность
09.02.07 Информационные системы и программирование

Якутск – 2024 г.

Материалы текущего контроля знаний и умений

Дайте определение и приведите примеры:

1. Абонент
2. Абонентское шифрование
3. Абстрактное представление данных
4. Аварийная ситуация
5. Аварийное завершение
6. Аварийный отказ
7. Автоматизированная информационная система, АИС
8. Автоматическая проверка
9. Автоматический верификатор
10. Автоматический контроль
11. Автономное /инженерное/ средство защиты информации
12. Авторизация
13. Авторизация данных
14. Авторизация программы
15. Авторское право
16. Администратор базы данных
17. Администратор доступа
18. Администратор защиты
19. Администратор системы
20. Администратор службы безопасности
21. Администрация банка данных
22. Администрация системы
23. Администрирование базы данных
24. Аккредитация
25. Аккредитация в области защиты информации
26. Активная угроза
27. Активное скрытие
28. Активное содержимое
29. Активное техническое средство защиты
30. Акустическая защита выделенного помещения
31. Акустическая защищенность выделенного помещения
32. Акустическая информация
33. Алгоритм
34. Алгоритм шифрования
35. Анализ затрат
36. Анализ прерывания
37. Анализ риска
38. Анализ трафика
39. Анализатор
40. Анализатор аварийного состояния
41. Анализатор прерываний
42. Антивирус
43. Аппаратная защита
44. Аппаратный контроль
45. Аппаратура засекречивания
46. Аппаратура технической разведки
47. Апплеты
48. Архив
49. Асимметричный шифр
50. Ассемблер
51. Атака
52. Атрибут
53. Атрибут файла
54. Аттестат выделенного помещения
55. Аттестат объекта защиты

56. Аттестация
57. Аттестация выделенного помещения
58. Аттестация защиты
59. Аттестация объекта защиты
60. Аттестация предприятий
61. Аттестация программы
62. Аттестация средств защиты
63. Аутентификатор
64. Аутентификация
65. Аутентификация данных
66. Аутентификация источника данных
67. Аутентификация пользователя
68. Аутентификация сообщений
69. База данных
70. Банк данных
71. Безопасная операционная система
72. Безопасное время
73. Безопасное состояние
74. Безопасность
75. Безопасность автоматизированной информационной системы
76. Безопасность данных
77. Безопасность информации
78. Безопасность информации в ИС
79. Безопасность информационной сети
80. Безопасность информационной системы
81. Безопасность компьютерных систем
82. Безопасность персонала
83. Безопасность предприятия
84. Безопасность связи
85. Безотказность
86. Белый /акустический/ шум
87. Биометрические данные
88. Бит (двоичный код)
89. Блок начальной загрузки
90. Блокирование информации
91. Блокировка доступа
92. Блокировка записи в память
93. Блокировка клавиатуры
94. Блокировка памяти
95. Блочный алгоритм шифрования
96. Брандмауэр
97. Брандмауэр с фильтрацией пакетов
98. Браузер
99. Ведение базы данных
100. Визуальный контроль
101. Вирус
102. Вирус невидимка
103. Владелец информации
104. Внешнее воздействие на информационный ресурс
105. Восстановление
106. Восстановление данных
107. Время доступа
108. Время жизни
109. Встроенный дешифратор
110. Вторичный ключ
111. Вычислительная сеть
112. Гамма шифра
113. Гаммирование

114. Гарантии
115. Гарантия защиты
116. Генератор
117. Генератор случайных паролей
118. Генератор случайных чисел
119. Государственная тайна
120. Датчик случайных чисел
121. Двоичный код с исправлением ошибок
122. Дезинформация
123. Декодирование
124. Дескриптор
125. Дешифратор
126. Дешифрование
127. Диагностика
128. Диспетчер доступа
129. Документ
130. Достоверное программное обеспечение
131. Доступ
132. Дыра
133. Журнал
134. Журнал восстановления
135. Журнал ошибок
136. Зависание программы
137. Зависание системы
138. Загрузка по линии связи
139. Загрузочный вирус
140. Закрытая информация
141. Заражение
142. Зарегистрированный пользователь
143. Зашифрованные данные
144. Защита выделенного помещения
145. Защита вычислительной сети
146. Защита информации
147. Защита объектов
148. Защита от несанкционированного доступа
149. Защита от копирования
150. Защита паролем
151. Защита программы
152. Злоумышленник
153. Злоумышленное использование вычислительной машины
154. Идентификатор пользователя
155. Идентификация
156. Избыточность
157. Изменение формата
158. Имитация
159. Имитозащита
160. Инсталляция
161. Интерпретация
162. Интерфейс
163. Информатизация
164. Информационная безопасность
165. Информационная система
166. Информационные ресурсы
167. Информация с ограниченным доступом
168. Искажение
169. Испытание на проникновение
170. Испытательная модель
171. Канал утечки акустической информации

172. Категория
173. Категория защиты
174. Класс защищенности средств вычислительной техники (автоматизированной системы)
175. Ключ
176. Код
177. Коллективный (групповой) доступ
178. Коммерческая тайна
179. Компилятор
180. Компрометация
181. Компьютерное преступление
182. Компьютерный вирус
183. Контроль доступа
184. Контрольная сумма
185. Контрольный код
186. Конфиденциальность
187. Концепция защиты информации
188. Концепция доступа
189. Криптоанализ
190. Криптографическая защита
191. Криптографическая проверка
192. Криптографическая система
193. Криптографический метод защиты информации
194. Криптографическое преобразование (информации)
195. Криптография
196. Лечение (выкусывание) [Cure]
197. Лицензионное соглашение /договор/ в области защиты информации
198. Лицензирование в области защиты информации
199. Лицензия
200. Личная безопасность
201. Личная информация
202. Логическая "бомба"
203. Мандат
204. Мандатное управление доступом
205. Матрица доступа
206. Матрица полномочий
207. Надежность
208. Нарушение полномочий
209. Нарушение целостности
210. Нарушитель
211. Нарушитель правил доступа
212. Непрерывность защиты
213. Нештатная ситуация
214. Обратный ассемблер
215. Обход системы
216. Орган по сертификации в области защиты информации
217. Организационная защита информации
218. Отказ
219. Отказ в обслуживании
220. Отказоустойчивая система
221. Открытый текст
222. Пароль
223. Патент
224. Перестановка
225. Перехват сообщений
226. Период доступа
227. Плагин
228. Побочное электромагнитное излучение (ПЭМИ)
229. Повреждение данных

230. Подстановка
231. Подтверждение подлинности
232. Политика информационной безопасности
233. Полномочия
234. Полномочное управление доступом
235. Получатель информации
236. Помехи
237. Помехозащищенность
238. Посредник [PROXY]
239. Почта электронная
240. Почтовые "бомбы"
241. Привилегии
242. Привилегированный пользователь
243. Программная закладка
244. Программная "бомба"
245. Проникновение
246. Протокол Telnet
247. Протокол безопасной передачи данных [SSL]
248. Протокол передачи файлов [FTP]
249. Разграничение доступа
250. Разрушение информации
251. Расшифрование
252. Режимное предприятие /учреждение/
253. Самокодирование
254. Самоконтроль
255. Санкционирование
256. Санкционированный доступ (к информации)
257. Сбой
258. Сбор данных
259. Секретная информация
260. Сервер-посредник[Proxy server]
261. Сигнализация
262. Система замков и ключей
263. Система защиты информации
264. Система защиты данных
265. Система кодирования
266. Система обработки данных
267. Системный журнал
268. Скрытие
269. Служба безопасности
270. Собственник информации
271. Спамминг
272. Средства восстановления
273. Средство криптографической защиты (информации)
274. Страховая форма защиты информации
275. Субъект
276. Считыватель карт
277. Толерантность
278. Трафик
279. Троянский конь
280. Угроза
281. Угроза безопасности информации
282. Уничтожение информации
283. Управление доступом
284. Управление информационной безопасностью
285. Уровень (технической) защиты информации
286. Уровень безопасности
287. Устройство стирания данных

288. Утечка /рассекречивание/ информации
289. Уязвимость
290. Уязвимые места
291. Фальсификация
292. Физическая безопасность
293. Хакер
294. Целостность
295. Ценность информации
296. Цифровая подпись
297. Червь
298. Шифр
299. Шифратор

Опишите порядок выполнения следующих действий:

1. С помощью OpenSSL сгенерируйте ключ шифрования для алгоритма DES.
2. С помощью OpenSSL примените ключ шифрования и алгоритм DES к текстовому файлу. Измерьте время шифрования.
3. Выполните шифрование по алгоритмам DES-EDE и 3DES, используя только функцию DES.
4. Сравните время шифрования с применением алгоритмов DES, DES-EDE, 3DES, RSA.
5. С помощью OpenSSL вычислите значение хэш-функции MD5 от подготовленного текста. Измерьте время хеширования.
6. С помощью OpenSSL вычислите значение хэш-функции SHA1 от подготовленного текста. Измерьте время хеширования.
7. Получите аутентификатор выбранного файла с применением алгоритма DES-CBC с помощью OpenSSL и вручную.
8. Посчитайте хеш-суммы MD5 и SHA1 от изменѐнного файла. Убедитесь, что значения сумм от исходного и изменѐнного файлов не совпадают.
9. Создайте запрос на сертификацию. Выведите запрос на сертификацию в текстовом виде, укажите назначение и смысл значения каждого поля.
10. Сгенерируйте ключ RSA и подпишите им созданный запрос, укажите формат сертификата DER.
11. Преобразуйте формат сертификата из DER в PEM. Покажите, что изменилось. Поясните разницу между DER и PEM.
12. С помощью OpenSSL создайте новый центр сертификации
13. Выпустите сертификат «A». Проверьте подлинность сертификата «A» с помощью сертификата удостоверяющего центра.
14. С помощью GnuPG выпустите по 3 пары ключей для подписи на каждом из компьютеров (A1, B1, C1, A2, B2, C2, A3, B3, C3).
15. Выстройте следующую сеть доверия (стрелкой обозначено направление доверия): A1 -> A2 -> C1 -> C3, B1 -> B2 -> A1, C1 -> B3 -> B2, A3 -> C2 -> A1.
16. Изменяя степени доверия к тем или иным сертификатам, вычислите вручную новые степени доверия в сети и проверьте свои расчѐты программой gpg2.
17. Создайте криптоконтейнер с файловой системой ext4, разместите в нём несколько файлов. Убедитесь, что после закрытия криптоконтейнера ни прочитать файлы, расположенные в нём, ни подключить его к файловой системе не удаётся.

Вопрос 1

Что НЕ относится к угрозам информационной безопасности ?

- классификация информации
- преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов)
- сбои и отказы оборудования (технических средств)

Вопрос 2

Какие действия НЕ относятся к реагированию на нарушение режима информационной безопасности организации?

- выявление нарушителя
- предупреждение повторных нарушений
- судебное рассмотрение

Вопрос 3

Шифрование с симметричным ключом предполагает, что ... ?

- используется один ключ
- оба ключа одинаковы
- используются два разных ключа

Вопрос 4

Что такое электронная цифровая подпись?

- электронный документ, достоверность которого подтверждена удостоверяющим центром
- набор цифр персонально закрепленных за пользователями, неразрешенных к использованию любыми другими пользователями
- реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе

Вопрос 5

К активным угрозам относятся:

- копирование информации
- разрушение или радиоэлектронное подавление линий связи, вывод из строя ПЭВМ или операционной системы
- попытка получения информации, циркулирующей в каналах связи, посредством их прослушивания

Вопрос 6

Информация может составлять коммерческую тайну, если:

- к ней нет свободного доступа на законном основании
- содержится в учредительных документах
- содержится в бухгалтерских балансах

Вопрос 7

Системой дистанционного банковского обслуживания (ДБО) юридических лиц является

- sms- банкинг
- интернет-банкинг
- клиент-банк

Вопрос 8

Угрозой безопасности автоматизированных банковских систем не является

- Хакерские атаки
- Фишинг
- Аутсорсинг

Вопрос 9

Программы, предназначенные для записи информации о нажатиях клавиш клавиатуры в специализированный журнал регистрации (Log-файл), который впоследствии изучается установившим программу злоумышленником называются

- кейлоггеры
- троянцы-бэкдоры
- malware

Вопрос 10

Что такое политика информационной безопасности организации

- совокупность механизмов компьютерных систем
- набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию
- инструкции администраторам по настройке информационных систем

Вопрос 11

Какие угрозы безопасности информации являются преднамеренными ?

- Некомпетентное использование средств защиты

- Поджог
- Неумышленное повреждение каналов связи

Вопрос 12

К понятию информационной безопасности НЕ относятся:

- надежность работы компьютера
- природоохранные мероприятия
- сохранность ценных данных

Вопрос 13

НЕ являются коммерческой тайной?

- сведения, содержащиеся в документах, дающих право заниматься предпринимательской деятельностью
- сведения о персонале предприятия
- сведения о научных разработках

Вопрос 14

Какие меры НЕ позволяют повысить надежность парольной защиты ?

- выбор простого пароля
- управление сроком действия паролей, их периодическая смена
- ограничение числа неудачных попыток входа в систему

Вопрос 15

Что такое несанкционированный доступ ?

- вход в систему без согласования с руководителем организации
- удаление не нужной информации
- доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа

Вопрос 16

Какой алгоритм шифрования используется в платёжных системах Яндекс.Деньги, Web-money и Cyberplat ?

- RSA
- DSA
- ECDSA

Вопрос 17

Хакерская атака - это..?

- использование информации на влияние на умы союзников и противников
- блокирование информации, преследующее цель получить экономическое превосходство
- попытка взлома компьютерной системы

Вопрос 18

Какой вирус из нижеперечисленных НЕ входит в класс классических вирусов?

- загрузочные вирусы
- сетевые черви
- файловые вирусы

Вопрос 19

В системах дистанционного банковского обслуживания (ДБО) используется следующий протокол, осуществляющий шифрование конфиденциальной информации

- https
- http
- ftp
- smtp

Вопрос 20

По числу компьютерных преступлений лидируют:

- информационные системы сельхозпредприятий
- корпоративные информационные системы в промышленности
- автоматизированные банковские системы

Вопрос 21

Информационное оружие - это ..?

- комплекс технических, программных и других средств, методов и технологий предназначенных для распространения выгодной информации и дезинформации в системе формирования общественного мнения
- комплекс индивидуального и общественного сознания
- комплекс нормативно-правовой документации

Вопрос 22

В политике безопасности основным принципом является усиление самого слабого звена ?

- да
- отчасти
- нет

Вопрос 23

Какие функции НЕ выполняет антивирусная защита?

- поиск и уничтожение неизвестных вирусов
- определения адреса отправителя вирусов
- поиск и уничтожение известных вирусов

Вопрос 24

Что такое государственная тайна ?

- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ
- все сведения, которые хранятся в государственных базах данных
- сведения о состоянии окружающей среды

Вопрос 25

В политике безопасности НЕ должно быть:

- разграничения прав доступа к ресурсам
- разделение обязанностей
- возможность перехода в небезопасное состояние

Вопрос 26

Правовое обеспечение информационной безопасности - это..?

- широкое использование технических средств защиты информации
- документированные сведения, лежащие в основе решения задач, обеспечивающих функционирование системы
- нормативные документы по ИБ, требования которых являются обязательными в рамках сферы действия каждого подразделения

Вопрос 27

Ботнеты - это…

- Сеть компьютеров, зараженных блоккерами
- Сеть компьютеров, зараженных вредоносной программой, позволяющей удаленно управлять зараженными компьютерами, называется
- Сеть компьютеров, распространяющих сетевые черви

Вопрос 28

К какой главе УК РФ относятся ст. 272, ст. 273, ст. 274 в области информационной безопасности?

- 27
- 28
- 25

Вопрос 29

Для компьютерных преступлений характерна:

- наличие достаточной следственной практики по раскрытию компьютерных преступлений в РФ
- высокая латентность

- простота сбора доказательств

Вопрос 30

Какая наиболее яркая черта вируса "сетевой червь"?

- распространяется по сети
- саморепликация
- распространяется через съемные носители

Вопрос 31

СВЕДЕНИЯ (СООБЩЕНИЯ, ДАННЫЕ) НЕЗАВИСИМО ОТ ФОРМЫ ИХ ПРЕДСТАВЛЕНИЯ:

- Информация
- Информационные технологии
- Информационная система
- Информационно-телекоммуникационная сеть
- Обладатель информации

Вопрос 32

ПРОЦЕССЫ, МЕТОДЫ ПОИСКА, СБОРА, ХРАНЕНИЯ, ОБРАБОТКИ, ПРЕДОСТАВЛЕНИЯ, РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ И СПОСОБЫ ОСУЩЕСТВЛЕНИЯ ТАКИХ ПРОЦЕССОВ И МЕТОДОВ:

- Информация
- Информационные технологии
- Информационная система
- Информационно-телекоммуникационная сеть
- Обладатель информации

Вопрос 33

ЛИЦО, САМОСТОЯТЕЛЬНО СОЗДАВШЕЕ ИНФОРМАЦИЮ ЛИБО ПОЛУЧИВШЕЕ НА ОСНОВАНИИ ЗАКОНА ИЛИ ДОГОВОРА ПРАВО РАЗРЕШАТЬ ИЛИ ОГРАНИЧИВАТЬ ДОСТУП К ИНФОРМАЦИИ:

- Источник информации
- Потребитель информации
- Уничтожитель информации
- Носитель информации
- Обладатель информации

Вопрос 34

ТЕХНОЛОГИЧЕСКАЯ СИСТЕМА, ПРЕДНАЗНАЧЕННАЯ ДЛЯ ПЕРЕДАЧИ ПО ЛИНИЯМ СВЯЗИ ИНФОРМАЦИИ, ДОСТУП К КОТОРОЙ ОСУЩЕСТВЛЯЕТСЯ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ ЭТО:

- База данных
- Информационная технология
- Информационная система
- Информационно-телекоммуникационная сеть
- Медицинская информационная система

Вопрос 35

ОБЯЗАТЕЛЬНОЕ ДЛЯ ВЫПОЛНЕНИЯ ЛИЦОМ, ПОЛУЧИВШИМ ДОСТУП К ОПРЕДЕЛЕННОЙ ИНФОРМАЦИИ, ТРЕБОВАНИЕ НЕ ПЕРЕДАВАТЬ ТАКУЮ ИНФОРМАЦИЮ ТРЕТЬИМ ЛИЦАМ БЕЗ СОГЛАСИЯ ЕЕ ОБЛАДАТЕЛЯ ЭТО:

- Электронное сообщение
- Распространение информации
- Предоставление информации
- Конфиденциальность информации
- Доступ к информации

Вопрос 36

ДЕЙСТВИЯ, НАПРАВЛЕННЫЕ НА ПОЛУЧЕНИЕ ИНФОРМАЦИИ НЕОПРЕДЕЛЕННЫМ КРУГОМ ЛИЦ ИЛИ ПЕРЕДАЧУ ИНФОРМАЦИИ НЕОПРЕДЕЛЕННОМУ КРУГУ ЛИЦ ЭТО:

- Уничтожение информации
- Распространение информации
- Предоставление информации
- Конфиденциальность информации
- Доступ к информации

Вопрос 37

ВОЗМОЖНОСТЬ ПОЛУЧЕНИЯ ИНФОРМАЦИИ И ЕЕ ИСПОЛЬЗОВАНИЯ ЭТО:

- Сохранение информации
- Распространение информации
- Предоставление информации
- Конфиденциальность информации
- Доступ к информации

Вопрос 38

ИНФОРМАЦИЯ, ПЕРЕДАННАЯ ИЛИ ПОЛУЧЕННАЯ ПОЛЬЗОВАТЕЛЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ:

- Электронное сообщение
- Информационное сообщение
- Текстовое сообщение
- Визуальное сообщение
- SMS-сообщение

Вопрос 39

ВСЕ КОМПОНЕНТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРЕДПРИЯТИЯ, В КОТОРОМ НАКАПЛИВАЮТСЯ И ОБРАБАТЫВАЮТСЯ ПЕРСОНАЛЬНЫЕ ДАННЫЕ ЭТО:

- Информационная система персональных данных
- База данных
- Централизованное хранилище данных
- Система Статэкспресс
- Сервер

Вопрос 40

К СВЕДЕНИЯМ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА, СОГЛАСНО УКАЗУ ПРЕЗИДЕНТА РФ ОТ 6 МАРТА 1997 Г., ОТНОСЯТСЯ:

- Информация о распространении программ
- Информация о лицензировании программного обеспечения
- Информация, размещаемая в газетах, Интернете
- Персональные данные
- Личная тайна

Вопрос 41

ОТНОШЕНИЯ, СВЯЗАННЫЕ С ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ, РЕГУЛИРУЮТСЯ ЗАКОНОМ…

- «Об информации, информационных технологиях»
- «О защите информации»
- Федеральным законом «О персональных данных»
- Федеральным законом «О конфиденциальной информации»
- «Об утверждении перечня сведений конфиденциального характера»

Вопрос 42

ДЕЙСТВИЯ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ (СОГЛАСНО ЗАКОНУ), ВКЛЮЧАЯ СБОР, СИСТЕМАТИЗАЦИЮ, НАКОПЛЕНИЕ, ХРАНЕНИЕ, ИСПОЛЬЗОВАНИЕ, РАСПРОСТРАНЕНИЕ И Т. Д ЭТО:

- «Исправление персональных данных»
- «Работа с персональными данными»
- «Преобразование персональных данных»
- «Обработка персональных данных»
- «Изменение персональных данных»

Вопрос 43

ДЕЙСТВИЯ, В РЕЗУЛЬТАТЕ КОТОРЫХ НЕВОЗМОЖНО ОПРЕДЕЛИТЬ ПРИНАДЛЕЖНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ КОНКРЕТНОМУ СУБЪЕКТУ ПЕРСОНАЛЬНЫХ ДАННЫХ:

- Выделение персональных данных
- Обеспечение безопасности персональных данных
- Деаутентификация
- Деавторизация
- Деперсонификация

Вопрос 44

ПО РЕЖИМУ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ ПОДРАЗДЕЛЯЮТСЯ НА:

- Многопользовательские

- Однопользовательские
- Без разграничения прав доступа
- С разграничением прав доступа
- Системы, не имеющие подключений

Вопрос 45

ПРОЦЕСС СООБЩЕНИЯ СУБЪЕКТОМ СВОЕГО ИМЕНИ ИЛИ НОМЕРА, С ЦЕЛЬЮ ПОЛУЧЕНИЯ ОПРЕДЕЛЁННЫХ ПОЛНОМОЧИЙ (ПРАВ ДОСТУПА) НА ВЫПОЛНЕНИЕ НЕКОТОРЫХ (РАЗРЕШЕННЫХ ЕМУ) ДЕЙСТВИЙ В СИСТЕМАХ С ОГРАНИЧЕННЫМ ДОСТУПОМ:

- Авторизация
- Аутентификация
- Обезличивание
- Деперсонализация
- Идентификация

Вопрос 46

ПРОЦЕДУРА ПРОВЕРКИ СООТВЕТСТВИЯ СУБЪЕКТА И ТОГО, ЗА КОГО ОН ПЫТАЕТСЯ СЕБЯ ВЫДАТЬ, С ПОМОЩЬЮ НЕКОЙ УНИКАЛЬНОЙ ИНФОРМАЦИИ:

- Авторизация
- Обезличивание
- Деперсонализация
- Аутентифика́ция
- Идентификация

Вопрос 47

ПРОЦЕСС, А ТАКЖЕ РЕЗУЛЬТАТ ПРОЦЕССА ПРОВЕРКИ НЕКОТОРЫХ ОБЯЗАТЕЛЬНЫХ ПАРАМЕТРОВ ПОЛЬЗОВАТЕЛЯ И, ПРИ УСПЕШНОСТИ, ПРЕДОСТАВЛЕНИЕ ЕМУ ОПРЕДЕЛЁННЫХ ПОЛНОМОЧИЙ НА ВЫПОЛНЕНИЕ НЕКОТОРЫХ (РАЗРЕШЕННЫХ ЕМУ) ДЕЙСТВИЙ В СИСТЕМАХ С ОГРАНИЧЕННЫМ ДОСТУПОМ

- Авториза́ция
- Идентификация
- Аутентификация
- Обезличивание
- Деперсонализация

Вопрос 48

ПРОСТЕЙШИМ СПОСОБОМ ИДЕНТИФИКАЦИИ В КОМПЬЮТЕРНОЙ СИСТЕМЕ ЯВЛЯЕТСЯ ВВОД ИДЕНТИФИКАТОРА ПОЛЬЗОВАТЕЛЯ, КОТОРЫЙ ИМЕЕТ СЛЕДУЮЩЕЕ НАЗВАНИЕ:

- Токен
- Password
- Пароль
- Login
- Смарт-карта

Вопрос 49

ОСНОВНОЕ СРЕДСТВО, ОБЕСПЕЧИВАЮЩЕЕ КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ, ПОСЫЛАЕМОЙ ПО ОТКРЫТЫМ КАНАЛАМ ПЕРЕДАЧИ ДАННЫХ, В ТОМ ЧИСЛЕ – ПО СЕТИ ИНТЕРНЕТ:

- Идентификация
- Аутентификация
- Авторизация
- Экспертиза
- Шифрование

Вопрос 50

ДЛЯ БЕЗОПАСНОЙ ПЕРЕДАЧИ ДАННЫХ ПО КАНАЛАМ ИНТЕРНЕТ ИСПОЛЬЗУЕТСЯ ТЕХНОЛОГИЯ:

- WWW
- DICOM
- VPN
- FTP
- XML

Вопрос 51

КОМПЛЕКС АППАРАТНЫХ И/ИЛИ ПРОГРАММНЫХ СРЕДСТВ, ОСУЩЕСТВЛЯЮЩИЙ КОНТРОЛЬ И ФИЛЬТРАЦИЮ СЕТЕВОГО ТРАФИКА В СООТВЕТСТВИИ С ЗАДАННЫМИ ПРАВИЛАМИ И

ЗАЩИЩАЮЩИЙ КОМПЬЮТЕРНЫЕ СЕТИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА:

- Антивирус
- Замок
- Брандма́уэр
- Криптография
- Экспертная система

Вопрос 52

ЗА ПРАВОНАРУШЕНИЯ В СФЕРЕ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ЗАЩИТЫ ИНФОРМАЦИИ ДАННЫЙ ВИД НАКАЗАНИЯ НА СЕГОДНЯШНИЙ ДЕНЬ НЕ ПРЕДУСМОТРЕН:

- Дисциплинарные взыскания
- Административный штраф
- Уголовная ответственность
- Лишение свободы
- Смертная казнь

Вопрос 53

НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К ИНФОРМАЦИИ ЭТО:

- Доступ к информации, не связанный с выполнением функциональных обязанностей и не оформленный документально
- Работа на чужом компьютере без разрешения его владельца
- Вход на компьютер с использованием данных другого пользователя
- Доступ к локально-информационной сети, связанный с выполнением функциональных обязанностей
- Доступ к СУБД под запрещенным именем пользователя

Вопрос 54

«ПЕРСОНАЛЬНЫЕ ДАННЫЕ» ЭТО:

- Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу
- Фамилия, имя, отчество физического лица
- Год, месяц, дата и место рождения, адрес физического лица
- Адрес проживания физического лица
- Сведения о семейном, социальном, имущественном положении человека, составляющие понятие «профессиональная тайна»

Вопрос 55

В ДАННОМ СЛУЧАЕ СОТРУДНИК УЧРЕЖДЕНИЯ МОЖЕТ БЫТЬ ПРИВЛЕЧЕН К ОТВЕТСТВЕННОСТИ ЗА НАРУШЕНИЯ ПРАВИЛ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ:

- Выход в Интернет без разрешения администратора
- При установке компьютерных игр
- В случаях установки нелицензионного ПО
- В случае не выхода из информационной системы
- В любом случае неправомочного использования конфиденциальной информации при условии письменного предупреждения сотрудника об ответственности

Вопрос 56

МОЖЕТ ЛИ СОТРУДНИК БЫТЬ ПРИВЛЕЧЕН К УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА НАРУШЕНИЯ ПРАВИЛ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ:

- Нет, только к административной ответственности
- Нет, если это государственное предприятие
- Да
- Да, но только в случае, если действия сотрудника нанесли непоправимый вред
- Да, но только в случае осознанных неправомочных действий сотрудника

Вопрос 57

ПРОЦЕДУРА, ПРОВЕРЯЮЩАЯ, ИМЕЕТ ЛИ ПОЛЬЗОВАТЕЛЬ С ПРЕДЪЯВЛЕННЫМ ИДЕНТИФИКАТОРОМ ПРАВО НА ДОСТУП К РЕСУРСУ ЭТО:

- Идентификация
- Аутентификация
- Стратификация
- Регистрация
- Авторизация

Вопрос 58

НАИБОЛЕЕ ОПАСНЫМ ИСТОЧНИКОМ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПРЕДПРИЯТИЯ ЯВЛЯЮТСЯ:

1. Другие предприятия (конкуренты)
2. Сотрудники информационной службы предприятия, имеющие полный доступ к его информационным ресурсам
3. Рядовые сотрудники предприятия
4. Возможные отказы оборудования, отключения электропитания, нарушения в сети передачи данных
5. Хакеры

Вопрос 59

ВЫБЕРИТЕ, МОЖНО ЛИ В СЛУЖЕБНЫХ ЦЕЛЯХ ИСПОЛЬЗОВАТЬ ЭЛЕКТРОННЫЙ АДРЕС (ПОЧТОВЫЙ ЯЩИК), ЗАРЕГИСТРИРОВАННЫЙ НА ОБЩЕДОСТУПНОМ ПОЧТОВОМ СЕРВЕРЕ, НАПРИМЕР НА MAIL.RU:

- Нет, не при каких обстоятельствах
- Нет, но для отправки срочных и особо важных писем можно
- Можно, если по нему пользователь будет пересылать информацию, не содержащую сведений конфиденциального характера
- Можно, если информацию предварительно заархивировать с помощью программы winrar с паролем
- Можно, если других способов электронной передачи данных на предприятии или у пользователя в настоящий момент нет, а информацию нужно переслать срочно

Вопрос 60

ДОКУМЕНТИРОВАННАЯ ИНФОРМАЦИЯ, ДОСТУП К КОТОРОЙ ОГРАНИЧИВАЕТ В СООТВЕТСТВИИ С ЗАКОНАДЕЛЬСТВОМ РФ:

- Информация составляющая государственную тайну
- Информация составляющая коммерческую тайну
- Персональная
- Конфиденциальная информация
- Документированная информация

Вопрос 61

ДЛЯ ТОГО ЧТОБЫ СНИЗИТЬ ВЕРОЯТНОСТЬ УТРАТЫ ИНФОРМАЦИИ НЕОБХОДИМО:

- Регулярно производить антивирусную проверку компьютера
- Регулярно выполнять проверку жестких дисков компьютера на наличие ошибок
- Регулярно копировать информацию на внешние носители (сервер, компакт-диски, флэш-карты)
- Защитить вход на компьютер к данным паролем
- Проводить периодическое обслуживание ПК

Вопрос 62

ПАРОЛЬ ПОЛЬЗОВАТЕЛЯ ДОЛЖЕН

- Содержать цифры и буквы, знаки препинания и быть сложным для угадывания
- Содержать только цифры
- Содержать только буквы
- Иметь явную привязку к владельцу (его имя, дата рождения, номер телефона и т.п.)
- Быть простым и легко запоминаться, например «123», «111», «qwerty» и т.д.

Вопрос 63

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЕСПЕЧИВАЕТ…

- Блокирование информации
- Искажение информации
- Сохранность информации
- Утрату информации
- Подделку информации

Вопрос 64

ЗАКОН РОССИЙСКОЙ ФЕДЕРАЦИИ «О ГОСУДАРСТВЕННОЙ ТАЙНЕ» БЫЛ ПРИНЯТ В СЛЕДУЮЩЕМ ГОДУ:

- 1982
- 1985
- 1988
- 1993
- 2005

Вопрос 65

ДОКУМЕНТИРОВАННОЙ ИНФОРМАЦИЕЙ, ДОСТУП К КОТОРОЙ ОГРАНИЧЕН В СООТВЕТСТВИИ С ЗАКОНОДАТЕЛЬСТВОМ РФ, НАЗЫВАЕТСЯ

- Конфиденциальная
- Персональная
- Документированная
- Информация составляющая государственную тайну
- Информация составляющая коммерческую тайну

Вопрос 66

ИНФОРМАЦИЯ ОБ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА ПРЕСТУПЛЕНИЕ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ОПИСАНА В:

- 1 главе Уголовного кодекса
- 5 главе Уголовного кодекса
- 28 главе Уголовного кодекса
- 100 главе Уголовного кодекса
- 1000 главе Уголовного кодекса

Вопрос 67

В СТАТЬЕ 272 УГОЛОВНОГО КОДЕКСА ГОВОРИТСЯ…

- О неправомерном доступе к компьютерной информации
- О создании, исполнении и распространении вредоносных программ для ЭВМ
- О нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети
- О преступлениях в сфере компьютерной информации
- Об ответственности за преступления в сфере компьютерной информации

Вопрос 68

ФЕДЕРАЛЬНЫЙ ЗАКОН «ОБ ИНФОРМАЦИИ, ИНФОРМАТИЗАЦИИ И ЗАЩИТЕ ИНФОРМАЦИИ» НАПРАВЛЕН НА:

- Регулирование взаимоотношений в информационной сфере совместно с гражданским кодексом РФ
- Регулирование взаимоотношений в гражданском обществе РФ
- Регулирование требований к работникам служб, работающих с информаций
- Формирование необходимых норм и правил работы с информацией
- Формирование необходимых норм и правил, связанных с защитой детей от информации

Вопрос 69

ХИЩЕНИЕ ИНФОРМАЦИИ – ЭТО…

- Несанкционированное копирование информации
- Утрата информации
- Блокирование информации
- Искажение информации
- Продажа информации

Вопрос 70

ВЛАДЕЛЬЦЕМ ИНФОРМАЦИИ ПЕРВОЙ КАТЕГОРИИ ЯВЛЯЕТСЯ…

- Государство
- Коммерческая организация
- Муниципальное учреждение
- Любой гражданин
- Группа лиц, имеющих общее дело

Вопрос 71

ВЛАДЕЛЬЦЕМ ИНФОРМАЦИИ ВТОРОЙ КАТЕГОРИИ ЯВЛЯЕТСЯ…

- Простые люди
- Государство
- Коммерческая организация
- Муниципальное учреждение
- Некоммерческая организация

Вопрос 72

ВЛАДЕЛЬЦЕМ ИНФОРМАЦИИ ТРЕТЬЕЙ КАТЕГОРИИ ЯВЛЯЕТСЯ…

- Люди
- Государство
- Муниципальное учреждение
- Учреждение
- Некоммерческая организация

Вопрос 73

ИНФОРМАЦИЕЙ, СОСТАВЛЯЮЩЕЙ ГОСУДАРСТВЕННУЮ ТАЙНУ, ВЛАДЕЮТ:

- Государство
- Только образовательные учреждения
- Только президиум Верховного Совета РФ
- Граждане Российской Федерации
- Только министерство здравоохранения

Вопрос 74

ИНФОРМАЦИЕЙ, СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ, ВЛАДЕЮТ:

- Государство
- Различные учреждения
- Государственная Дума
- Граждане Российской Федерации
- Медико-социальные организации

Вопрос 75

ПЕРСОНАЛЬНЫМИ ДАННЫМИ ВЛАДЕЮТ:

- Государство
- Различные учреждения
- Государственная Дума
- Жители Российской Федерации
- Медико-социальные организации

Вопрос 76

ДОСТУП К ИНФОРМАЦИИ – ЭТО:

- Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя
- Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц
- Действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц
- Информация, переданная или полученная пользователем информационно-телекоммуникационной сети
- Возможность получения информации и ее использования

Вопрос 77

ДОКУМЕНТИРОВАННАЯ ИНФОРМАЦИЯ, ДОСТУП К КОТОРОЙ ОГРАНИЧИВАЕТСЯ В СООТВЕТСТВИИ С ЗАКОНОДАТЕЛЬСТВОМ РОССИЙСКОЙ ФЕДЕРАЦИИ ЭТО:

- Конфиденциальная информация
- Документы офера и договоров
- Факс
- Личный дневник
- Законы РФ

Вопрос 78

ПЛАСТИКОВАЯ КАРТОЧКА, СОДЕРЖАЩАЯ ЧИП ДЛЯ КРИПТОГРАФИЧЕСКИХ ВЫЧИСЛЕНИЙ И ВСТРОЕННУЮ ЗАЩИЩЕННУЮ ПАМЯТЬ ДЛЯ ХРАНЕНИЯ ИНФОРМАЦИИ:

- Токен
- Password
- Пароль
- Login
- Смарт-карта

Вопрос 79

УСТРОЙСТВО ДЛЯ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ, ПРЕДСТАВЛЯЮЩЕЕ СОБОЙ МОБИЛЬНОЕ ПЕРСОНАЛЬНОЕ УСТРОЙСТВО, НАПОМИНАЮЩИЕ МАЛЕНЬКИЙ ПЕЙДЖЕР, НЕ ПОДСОЕДИНЯЕМЫЕ К КОМПЬЮТЕРУ И ИМЕЮЩИЕ СОБСТВЕННЫЙ ИСТОЧНИК ПИТАНИЯ:

- Токен
- Автономный токен
- USB-токен
- Устройство iButton
- Смарт-карта

Вопрос 80

ДОСТУП ПОЛЬЗОВАТЕЛЯ К ИНФОРМАЦИОННЫМ РЕСУРСАМ КОМПЬЮТЕРА И / ИЛИ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ПРЕДПРИЯТИЯ ДОЛЖЕН РАЗРЕШАТЬСЯ ТОЛЬКО ПОСЛЕ:

- Включения компьютера
- Идентификации по логину и паролю
- Запроса паспортных данных
- Запроса доменного имени
- Запроса ФИО

Вопрос 81

АППАРАТНЫЕ МОДУЛИ ДОВЕРЕННОЙ ЗАГРУЗКИ «АККОРД - АМДЗ» ПРЕДСТАВЛЯЮТ СОБОЙ…

- Аппаратный контролер
- Электронный замок
- Система контроля
- Сетевой адаптер
- Копировальный аппарат

Вопрос 82

ЭЛЕКТРОННЫЕ ЗАМКИ «СОБОЛЬ» ПРЕДНАЗНАЧЕНЫ ДЛЯ …

- Обеспечения доверенной загрузки компьютера и контроля целостности файлов в системах
- Сканирования отпечатков пальцев
- Проверки скорости и загрузки файлов
- Общего контроля
- Идентификации пользователя

Вопрос 83

Для защиты от злоумышленников необходимо использовать:

- Системное программное обеспечение
- Прикладное программное обеспечение
- Антивирусные программы
- Компьютерные игры
- Музыку, видеофильмы

Вопрос 84

ФЕДЕРАЛЬНЫЙ ЗАКОН "ОБ ИНФОРМАЦИИ, ИНФОРМАТИЗАЦИИ И ЗАЩИТЕ ИНФОРМАЦИИ" ДАЕТ ОПРЕДЕЛЕНИЕ ИНФОРМАЦИИ:

- Текст книги или письма
- Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления
- Сведения о явлениях и процессах
- Факты и идеи в формализованном виде
- Шифрованный текст, текст на неизвестном языке

Вопрос 85

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЕСТЬ ОБЕСПЕЧЕНИЕ…

- Независимости информации
- Изменения информации
- Копирования информации
- Сохранности информации
- Преобразования информации

Показатели, критерии и шкала оценивания компетенций промежуточной аттестации знаний по учебной дисциплине «Информационная безопасность»

На основе типовых заданий формируются в автоматическом режиме тестовые задания для студентов: три вопроса из блока 1, три вопроса из блока 2 и четыре вопроса из блока 3. Программный комплекс формирует индивидуальные задания для каждого зарегистрированного в системе студента и устанавливает время прохождения тестирования. Результатом тестирования является процент правильных ответов, с учетом индивидуального семестрового рейтинга студента формируется оценка.

Максимальное количество баллов, которое студент может получить на экзамене, в соответствии с Положением составляет 40 баллов.

Оценка в баллах	Критерии оценивания компетенций
30-40 баллов	Студент глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать

	теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач, подтверждает полное освоение компетенций, предусмотренных программой экзамена.
20-29 баллов	Студент твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения, допуская некоторые неточности; демонстрирует хороший уровень освоения материала, информационной и коммуникативной культуры и в целом подтверждает освоение компетенций, предусмотренных программой экзамена.
10-19 баллов	Студент показывает знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, в целом, не препятствует усвоению последующего программного материала, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ, подтверждает освоение компетенций, предусмотренных программой экзамена на минимально допустимом уровне.
Менее 10 баллов	Студент не знает значительной части программного материала (менее 50% правильно выполненных заданий от общего объема работы), допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы, не подтверждает освоение компетенций, предусмотренных программой экзамена.

МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«АРКТИЧЕСКИЙ ГОСУДАРСТВЕННЫЙ АГРОТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО Арктический ГАТУ)
Колледж технологий и управления

Комплект материалов
для проведения контрольных работ
ОП.13 Информационная безопасность

09.02.07 Информационные системы и программирование

Якутск – 2024 г.

Типовые задания для оценки освоения учебной дисциплины

Блок 2 (уметь).

Опишите порядок выполнения следующих действий:

1. С помощью OpenSSL сгенерируйте ключ шифрования для алгоритма DES.
2. С помощью OpenSSL примените ключ шифрования и алгоритм DES к текстовому файлу. Измерьте время шифрования.
3. Выполните шифрование по алгоритмам DES-EDE и 3DES, используя только функцию DES.
4. Сравните время шифрования с применением алгоритмов DES, DES-EDE, 3DES, RSA.
5. С помощью OpenSSL вычислите значение хэш-функции MD5 от подготовленного текста. Измерьте время хеширования.
6. С помощью OpenSSL вычислите значение хэш-функции SHA1 от подготовленного текста. Измерьте время хеширования.
7. Получите аутентификатор выбранного файла с применением алгоритма DES-CBC с помощью OpenSSL и вручную.
8. Посчитайте хеш-суммы MD5 и SHA1 от изменѐнного файла. Убедитесь, что значения сумм от исходного и изменѐнного файлов не совпадают.
9. Создайте запрос на сертификацию. Выведите запрос на сертификацию в текстовом виде, укажите назначение и смысл значения каждого поля.
10. Сгенерируйте ключ RSA и подпишите им созданный запрос, укажите формат сертификата DER.
11. Преобразуйте формат сертификата из DER в PEM. Покажите, что изменилось. Поясните разницу между DER и PEM.
12. С помощью OpenSSL создайте новый центр сертификации
13. Выпустите сертификат «A». Проверьте подлинность сертификата «A» с помощью сертификата удостоверяющего центра.
14. С помощью GnuPG выпустите по 3 пары ключей для подписи на каждом из компьютеров (A1, B1, C1, A2, B2, C2, A3, B3, C3).
15. Выстройте следующую сеть доверия (стрелкой обозначено направление доверия): A1 -> A2 -> C1 -> C3, B1 -> B2 -> A1, C1 -> B3 -> B2, A3 -> C2 -> A1.
16. Изменяя степени доверия к тем или иным сертификатам, вычислите вручную новые степени доверия в сети и проверьте свои расчѐты программой gpg2.
17. Создайте криптоконтейнер с файловой системой ext4, разместите в нём несколько файлов. Убедитесь, что после закрытия криптоконтейнера ни прочитать файлы, расположенные в нём, ни подключить его к файловой системе не удаётся.

Блок 3 (владеть).

Вопрос 1

Что НЕ относится к угрозам информационной безопасности ?

- классификация информации
- преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов)
- сбои и отказы оборудования (технических средств)

Вопрос 2

Какие действия НЕ относятся к реагированию на нарушение режима информационной безопасности организации?

- выявление нарушителя
- предупреждение повторных нарушений
- судебное рассмотрение

Вопрос 3

Шифрование с симметричным ключом предполагает, что ... ?

- используется один ключ
- оба ключа одинаковы
- используются два разных ключа

Вопрос 4

Что такое электронная цифровая подпись?

- электронный документ, достоверность которого подтверждена удостоверяющим центром
- набор цифр персонально закрепленных за пользователями, неразрешенных к использованию любыми другими пользователями
- реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе

Вопрос 5

К активным угрозам относятся:

- копирование информации
- разрушение или радиоэлектронное подавление линий связи, вывод из строя ПЭВМ или операционной системы
- попытка получения информации, циркулирующей в каналах связи, посредством их прослушивания

Вопрос 6

Информация может составлять коммерческую тайну, если:

- к ней нет свободного доступа на законном основании
- содержится в учредительных документах
- содержится в бухгалтерских балансах

Вопрос 7

Системой дистанционного банковского обслуживания (ДБО) юридических лиц является

- sms- банкинг
- интернет-банкинг
- клиент-банк

Вопрос 8

Угрозой безопасности автоматизированных банковских систем не является

- Хакерские атаки
- Фишинг
- Аутсорсинг

Вопрос 9

Программы, предназначенные для записи информации о нажатиях клавиш клавиатуры в специализированный журнал регистрации (Log-файл), который впоследствии изучается установившим программу злоумышленником называются

- кейлоггеры
- троянцы-бэкдоры
- malware

Вопрос 10

Что такое политика информационной безопасности организации

- совокупность механизмов компьютерных систем
- набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию
- инструкции администраторам по настройке информационных систем

Вопрос 11

Какие угрозы безопасности информации являются преднамеренными ?

- Некомпетентное использование средств защиты
- Поджог
- Неумышленное повреждение каналов связи

Вопрос 12

К понятию информационной безопасности НЕ относятся:

- надежность работы компьютера

- природоохранные мероприятия
- сохранность ценных данных

Вопрос 13

НЕ являются коммерческой тайной?

- сведения, содержащиеся в документах, дающих право заниматься предпринимательской деятельностью
- сведения о персонале предприятия
- сведения о научных разработках

Вопрос 14

Какие меры НЕ позволяют повысить надежность парольной защиты ?

- выбор простого пароля
- управление сроком действия паролей, их периодическая смена
- ограничение числа неудачных попыток входа в систему

Вопрос 15

Что такое несанкционированный доступ ?

- вход в систему без согласования с руководителем организации
- удаление не нужной информации
- доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа

Вопрос 16

Какой алгоритм шифрования используется в платёжных системах Яндекс.Деньги, Web-money и Cyberplat ?

- RSA
- DSA
- ECDSA

Вопрос 17

Хакерская атака - это..?

- использование информации на влияние на умы союзников и противников
- блокирование информации, преследующее цель получить экономическое превосходство
- попытка взлома компьютерной системы

Вопрос 18

Какой вирус из нижеперечисленных НЕ входит в класс классических вирусов?

- загрузочные вирусы
- сетевые черви
- файловые вирусы

Вопрос 19

В системах дистанционного банковского обслуживания (ДБО) используется следующий протокол, осуществляющий шифрование конфиденциальной информации

- https
- http
- ftp
- smtp

Вопрос 20

По числу компьютерных преступлений лидируют:

- информационные системы сельхозпредприятий
- корпоративные информационные системы в промышленности
- автоматизированные банковские системы

Вопрос 21

Информационное оружие - это ..?

- комплекс технических, программных и других средств, методов и технологий предназначенных для распространения выгодной информации и дезинформации в системе формирования общественного мнения
- комплекс индивидуального и общественного сознания

- комплекс нормативно-правовой документации

Вопрос 22

В политике безопасности основным принципом является усиление самого слабого звена ?

- да
- отчасти
- нет

Вопрос 23

Какие функции НЕ выполняет антивирусная защита?

- поиск и уничтожение неизвестных вирусов
- определения адреса отправителя вирусов
- поиск и уничтожение известных вирусов

Вопрос 24

Что такое государственная тайна ?

- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ
- все сведения, которые хранятся в государственных базах данных
- сведения о состоянии окружающей среды

Вопрос 25

В политике безопасности НЕ должно быть:

- разграничения прав доступа к ресурсам
- разделение обязанностей
- возможность перехода в небезопасное состояние

Вопрос 26

Правовое обеспечение информационной безопасности - это..?

- широкое использование технических средств защиты информации
- документированные сведения, лежащие в основе решения задач, обеспечивающих функционирование системы
- нормативные документы по ИБ, требования которых являются обязательными в рамках сферы действия каждого подразделения

Вопрос 27

Ботнеты - это…

- Сеть компьютеров, зараженных блоккерами
- Сеть компьютеров, зараженных вредоносной программой, позволяющей удаленно управлять зараженными компьютерами, называется
- Сеть компьютеров, распространяющих сетевые черви

Вопрос 28

К какой главе УК РФ относятся ст. 272, ст. 273, ст. 274 в области информационной безопасности?

- 27
- 28
- 25

Вопрос 29

Для компьютерных преступлений характерна:

- наличие достаточной следственной практики по раскрытию компьютерных преступлений в РФ
- высокая латентность
- простота сбора доказательств

Вопрос 30

Какая наиболее яркая черта вируса "сетевой червь"?

- распространяется по сети
- саморепликация

- распространяется через съемные носители

Вопрос 31

СВЕДЕНИЯ (СООБЩЕНИЯ, ДАННЫЕ) НЕЗАВИСИМО ОТ ФОРМЫ ИХ ПРЕДСТАВЛЕНИЯ:

- Информация
- Информационные технологии
- Информационная система
- Информационно-телекоммуникационная сеть
- Обладатель информации

Вопрос 32

ПРОЦЕССЫ, МЕТОДЫ ПОИСКА, СБОРА, ХРАНЕНИЯ, ОБРАБОТКИ, ПРЕДОСТАВЛЕНИЯ, РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ И СПОСОБЫ ОСУЩЕСТВЛЕНИЯ ТАКИХ ПРОЦЕССОВ И МЕТОДОВ:

- Информация
- Информационные технологии
- Информационная система
- Информационно-телекоммуникационная сеть
- Обладатель информации

Вопрос 33

ЛИЦО, САМОСТОЯТЕЛЬНО СОЗДАВШЕЕ ИНФОРМАЦИЮ ЛИБО ПОЛУЧИВШЕЕ НА ОСНОВАНИИ ЗАКОНА ИЛИ ДОГОВОРА ПРАВО РАЗРЕШАТЬ ИЛИ ОГРАНИЧИВАТЬ ДОСТУП К ИНФОРМАЦИИ:

- Источник информации
- Потребитель информации
- Уничтожитель информации
- Носитель информации
- Обладатель информации

Вопрос 34

ТЕХНОЛОГИЧЕСКАЯ СИСТЕМА, ПРЕДНАЗНАЧЕННАЯ ДЛЯ ПЕРЕДАЧИ ПО ЛИНИЯМ СВЯЗИ ИНФОРМАЦИИ, ДОСТУП К КОТОРОЙ ОСУЩЕСТВЛЯЕТСЯ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ ЭТО:

- База данных
- Информационная технология
- Информационная система
- Информационно-телекоммуникационная сеть
- Медицинская информационная система

Вопрос 35

ОБЯЗАТЕЛЬНОЕ ДЛЯ ВЫПОЛНЕНИЯ ЛИЦОМ, ПОЛУЧИВШИМ ДОСТУП К ОПРЕДЕЛЕННОЙ ИНФОРМАЦИИ, ТРЕБОВАНИЕ НЕ ПЕРЕДАВАТЬ ТАКУЮ ИНФОРМАЦИЮ ТРЕТЬИМ ЛИЦАМ БЕЗ СОГЛАСИЯ ЕЕ ОБЛАДАТЕЛЯ ЭТО:

- Электронное сообщение
- Распространение информации
- Предоставление информации
- Конфиденциальность информации
- Доступ к информации

Вопрос 36

ДЕЙСТВИЯ, НАПРАВЛЕННЫЕ НА ПОЛУЧЕНИЕ ИНФОРМАЦИИ НЕОПРЕДЕЛЕННЫМ КРУГОМ ЛИЦ ИЛИ ПЕРЕДАЧУ ИНФОРМАЦИИ НЕОПРЕДЕЛЕННОМУ КРУГУ ЛИЦ ЭТО:

- Уничтожение информации
- Распространение информации
- Предоставление информации
- Конфиденциальность информации
- Доступ к информации

Вопрос 37

ВОЗМОЖНОСТЬ ПОЛУЧЕНИЯ ИНФОРМАЦИИ И ЕЕ ИСПОЛЬЗОВАНИЯ ЭТО:

- Сохранение информации
- Распространение информации
- Предоставление информации
- Конфиденциальность информации
- Доступ к информации

Вопрос 38

ИНФОРМАЦИЯ, ПЕРЕДАННАЯ ИЛИ ПОЛУЧЕННАЯ ПОЛЬЗОВАТЕЛЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ:

- Электронное сообщение
- Информационное сообщение
- Текстовое сообщение
- Визуальное сообщение
- SMS-сообщение

Вопрос 39

ВСЕ КОМПОНЕНТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРЕДПРИЯТИЯ, В КОТОРОМ НАКАПЛИВАЮТСЯ И ОБРАБАТЫВАЮТСЯ ПЕРСОНАЛЬНЫЕ ДАННЫЕ ЭТО:

- Информационная система персональных данных
- База данных
- Централизованное хранилище данных
- Система Статэкспресс
- Сервер

Вопрос 40

К СВЕДЕНИЯМ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА, СОГЛАСНО УКАЗУ ПРЕЗИДЕНТА РФ ОТ 6 МАРТА 1997 Г., ОТНОСЯТСЯ:

- Информация о распространении программ
- Информация о лицензировании программного обеспечения
- Информация, размещаемая в газетах, Интернете
- Персональные данные
- Личная тайна

Вопрос 41

ОТНОШЕНИЯ, СВЯЗАННЫЕ С ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ, РЕГУЛИРУЮТСЯ ЗАКОНОМ…

- «Об информации, информационных технологиях»
- «О защите информации»
- Федеральным законом «О персональных данных»
- Федеральным законом «О конфиденциальной информации»
- «Об утверждении перечня сведений конфиденциального характера»

Вопрос 42

ДЕЙСТВИЯ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ (СОГЛАСНО ЗАКОНУ), ВКЛЮЧАЯ СБОР, СИСТЕМАТИЗАЦИЮ, НАКОПЛЕНИЕ, ХРАНЕНИЕ, ИСПОЛЬЗОВАНИЕ, РАСПРОСТРАНЕНИЕ И Т. Д ЭТО:

- «Исправление персональных данных»
- «Работа с персональными данными»
- «Преобразование персональных данных»
- «Обработка персональных данных»
- «Изменение персональных данных»

Вопрос 43

ДЕЙСТВИЯ, В РЕЗУЛЬТАТЕ КОТОРЫХ НЕВОЗМОЖНО ОПРЕДЕЛИТЬ ПРИНАДЛЕЖНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ КОНКРЕТНОМУ СУБЪЕКТУ ПЕРСОНАЛЬНЫХ ДАННЫХ:

- Выделение персональных данных
- Обеспечение безопасности персональных данных
- Деаутентификация
- Деавторизация
- Деперсонификация

Вопрос 44

ПО РЕЖИМУ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ ПОДРАЗДЕЛЯЮТСЯ НА:

- Многопользовательские
- Однопользовательские
- Без разграничения прав доступа
- С разграничением прав доступа
- Системы, не имеющие подключений

Вопрос 45

ПРОЦЕСС СООБЩЕНИЯ СУБЪЕКТОМ СВОЕГО ИМЕНИ ИЛИ НОМЕРА, С ЦЕЛЬЮ ПОЛУЧЕНИЯ

ОПРЕДЕЛЁННЫХ ПОЛНОМОЧИЙ (ПРАВ ДОСТУПА) НА ВЫПОЛНЕНИЕ НЕКОТОРЫХ (РАЗРЕШЕННЫХ ЕМУ) ДЕЙСТВИЙ В СИСТЕМАХ С ОГРАНИЧЕННЫМ ДОСТУПОМ:

- Авторизация
- Аутентификация
- Обезличивание
- Деперсонализация
- Идентификация

Вопрос 46

ПРОЦЕДУРА ПРОВЕРКИ СООТВЕТСТВИЯ СУБЪЕКТА И ТОГО, ЗА КОГО ОН ПЫТАЕТСЯ СЕБЯ ВЫДАТЬ, С ПОМОЩЬЮ НЕКОЙ УНИКАЛЬНОЙ ИНФОРМАЦИИ:

- Авторизация
- Обезличивание
- Деперсонализация
- Аутентифика́ция
- Идентификация

Вопрос 47

ПРОЦЕСС, А ТАКЖЕ РЕЗУЛЬТАТ ПРОЦЕССА ПРОВЕРКИ НЕКОТОРЫХ ОБЯЗАТЕЛЬНЫХ ПАРАМЕТРОВ ПОЛЬЗОВАТЕЛЯ И, ПРИ УСПЕШНОСТИ, ПРЕДОСТАВЛЕНИЕ ЕМУ ОПРЕДЕЛЁННЫХ ПОЛНОМОЧИЙ НА ВЫПОЛНЕНИЕ НЕКОТОРЫХ (РАЗРЕШЕННЫХ ЕМУ) ДЕЙСТВИЙ В СИСТЕМАХ С ОГРАНИЧЕННЫМ ДОСТУПОМ

- Авториза́ция
- Идентификация
- Аутентификация
- Обезличивание
- Деперсонализация

Вопрос 48

ПРОСТЕЙШИМ СПОСОБОМ ИДЕНТИФИКАЦИИ В КОМПЬЮТЕРНОЙ СИСТЕМЕ ЯВЛЯЕТСЯ ВВОД ИДЕНТИФИКАТОРА ПОЛЬЗОВАТЕЛЯ, КОТОРЫЙ ИМЕЕТ СЛЕДУЮЩЕЕ НАЗВАНИЕ:

- Токен
- Password
- Пароль
- Login
- Смарт-карта

Вопрос 49

ОСНОВНОЕ СРЕДСТВО, ОБЕСПЕЧИВАЮЩЕЕ КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ, ПОСЫЛАЕМОЙ ПО ОТКРЫТЫМ КАНАЛАМ ПЕРЕДАЧИ ДАННЫХ, В ТОМ ЧИСЛЕ – ПО СЕТИ ИНТЕРНЕТ:

- Идентификация
- Аутентификация
- Авторизация
- Экспертиза
- Шифрование

Вопрос 50

ДЛЯ БЕЗОПАСНОЙ ПЕРЕДАЧИ ДАННЫХ ПО КАНАЛАМ ИНТЕРНЕТ ИСПОЛЬЗУЕТСЯ ТЕХНОЛОГИЯ:

- WWW
- DICOM
- VPN
- FTP
- XML

Вопрос 51

КОМПЛЕКС АППАРАТНЫХ И/ИЛИ ПРОГРАММНЫХ СРЕДСТВ, ОСУЩЕСТВЛЯЮЩИЙ КОНТРОЛЬ И ФИЛЬТРАЦИЮ СЕТЕВОГО ТРАФИКА В СООТВЕТСТВИИ С ЗАДАННЫМИ ПРАВИЛАМИ И ЗАЩИЩАЮЩИЙ КОМПЬЮТЕРНЫЕ СЕТИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА:

- Антивирус
- Замок
- Брандма́уэр
- Криптография
- Экспертная система

Вопрос 52

ЗА ПРАВОНАРУШЕНИЯ В СФЕРЕ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ЗАЩИТЫ ИНФОРМАЦИИ ДАННЫЙ ВИД НАКАЗАНИЯ НА СЕГОДНЯШНИЙ ДЕНЬ НЕ ПРЕДУСМОТРЕН:

- Дисциплинарные взыскания
- Административный штраф
- Уголовная ответственность
- Лишение свободы
- Смертная казнь

Вопрос 53

НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К ИНФОРМАЦИИ ЭТО:

- Доступ к информации, не связанный с выполнением функциональных обязанностей и не оформленный документально
- Работа на чужом компьютере без разрешения его владельца
- Вход на компьютер с использованием данных другого пользователя
- Доступ к локально-информационной сети, связанный с выполнением функциональных обязанностей
- Доступ к СУБД под запрещенным именем пользователя

Вопрос 54

«ПЕРСОНАЛЬНЫЕ ДАННЫЕ» ЭТО:

- Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу
- Фамилия, имя, отчество физического лица
- Год, месяц, дата и место рождения, адрес физического лица
- Адрес проживания физического лица
- Сведения о семейном, социальном, имущественном положении человека, составляющие понятие «профессиональная тайна»

Вопрос 55

В ДАННОМ СЛУЧАЕ СОТРУДНИК УЧРЕЖДЕНИЯ МОЖЕТ БЫТЬ ПРИВЛЕЧЕН К ОТВЕТСТВЕННОСТИ ЗА НАРУШЕНИЯ ПРАВИЛ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ:

- Выход в Интернет без разрешения администратора
- При установке компьютерных игр
- В случаях установки нелицензионного ПО
- В случае не выхода из информационной системы
- В любом случае неправомочного использования конфиденциальной информации при условии письменного предупреждения сотрудника об ответственности

Вопрос 56

МОЖЕТ ЛИ СОТРУДНИК БЫТЬ ПРИВЛЕЧЕН К УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА НАРУШЕНИЯ ПРАВИЛ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ:

- Нет, только к административной ответственности
- Нет, если это государственное предприятие
- Да
- Да, но только в случае, если действия сотрудника нанесли непоправимый вред
- Да, но только в случае осознанных неправомочных действий сотрудника

Вопрос 57

ПРОЦЕДУРА, ПРОВЕРЯЮЩАЯ, ИМЕЕТ ЛИ ПОЛЬЗОВАТЕЛЬ С ПРЕДЪЯВЛЕННЫМ ИДЕНТИФИКАТОРОМ ПРАВО НА ДОСТУП К РЕСУРСУ ЭТО:

- Идентификация
- Аутентификация
- Стратификация
- Регистрация
- Авторизация

Вопрос 58

НАИБОЛЕЕ ОПАСНЫМ ИСТОЧНИКОМ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ ЯВЛЯЮТСЯ:

1. Другие предприятия (конкуренты)
2. Сотрудники информационной службы предприятия, имеющие полный доступ к его информационным ресурсам
3. Рядовые сотрудники предприятия
4. Возможные отказы оборудования, отключения электропитания, нарушения в сети передачи данных

5. Хакеры

Вопрос 59

ВЫБЕРИТЕ, МОЖНО ЛИ В СЛУЖЕБНЫХ ЦЕЛЯХ ИСПОЛЬЗОВАТЬ ЭЛЕКТРОННЫЙ АДРЕС (ПОЧТОВЫЙ ЯЩИК), ЗАРЕГИСТРИРОВАННЫЙ НА ОБЩЕДОСТУПНОМ ПОЧТОВОМ СЕРВЕРЕ, НАПРИМЕР НА MAIL.RU:

- Нет, не при каких обстоятельствах
- Нет, но для отправки срочных и особо важных писем можно
- Можно, если по нему пользователь будет пересылать информацию, не содержащую сведений конфиденциального характера
- Можно, если информацию предварительно заархивировать с помощью программы winrar с паролем
- Можно, если других способов электронной передачи данных на предприятии или у пользователя в настоящий момент нет, а информацию нужно переслать срочно

Вопрос 60

ДОКУМЕНТИРОВАННАЯ ИНФОРМАЦИЯ, ДОСТУП К КОТОРОЙ ОГРАНИЧИВАЕТ В СООТВЕТСТВИИ С ЗАКОНАДЕЛЬСТВОМ РФ:

- Информация составляющая государственную тайну
- Информация составляющая коммерческую тайну
- Персональная
- Конфиденциальная информация
- Документированная информация

Вопрос 61

ДЛЯ ТОГО ЧТОБЫ СНИЗИТЬ ВЕРОЯТНОСТЬ УТРАТЫ ИНФОРМАЦИИ НЕОБХОДИМО:

- Регулярно производить антивирусную проверку компьютера
- Регулярно выполнять проверку жестких дисков компьютера на наличие ошибок
- Регулярно копировать информацию на внешние носители (сервер, компакт-диски, флэш-карты)
- Защитить вход на компьютер к данным паролем
- Проводить периодическое обслуживание ПК

Вопрос 62

ПАРОЛЬ ПОЛЬЗОВАТЕЛЯ ДОЛЖЕН

- Содержать цифры и буквы, знаки препинания и быть сложным для угадывания
- Содержать только цифры
- Содержать только буквы
- Иметь явную привязку к владельцу (его имя, дата рождения, номер телефона и т.п.)
- Быть простым и легко запоминаться, например «123», «111», «qwerty» и т.д.

Вопрос 63

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЕСПЕЧИВАЕТ…

- Блокирование информации
- Искажение информации
- Сохранность информации
- Утрату информации
- Подделку информации

Вопрос 64

ЗАКОН РОССИЙСКОЙ ФЕДЕРАЦИИ «О ГОСУДАРСТВЕННОЙ ТАЙНЕ» БЫЛ ПРИНЯТ В СЛЕДУЮЩЕМ ГОДУ:

- 1982
- 1985
- 1988
- 1993
- 2005

Вопрос 65

ДОКУМЕНТИРОВАННОЙ ИНФОРМАЦИЕЙ, ДОСТУП К КОТОРОЙ ОГРАНИЧЕН В СООТВЕТСТВИИ С ЗАКОНОДАТЕЛЬСТВОМ РФ, НАЗЫВАЕТСЯ

- Конфиденциальная
- Персональная
- Документированная
- Информация составляющая государственную тайну
- Информация составляющая коммерческую тайну

Вопрос 66

ИНФОРМАЦИЯ ОБ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА ПРЕСТУПЛЕНИЕ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ОПИСАНА В:

- 1 главе Уголовного кодекса
- 5 главе Уголовного кодекса
- 28 главе Уголовного кодекса
- 100 главе Уголовного кодекса
- 1000 главе Уголовного кодекса

Вопрос 67

В СТАТЬЕ 272 УГОЛОВНОГО КОДЕКСА ГОВОРИТСЯ…

- О неправомерном доступе к компьютерной информации
- О создании, исполнении и распространении вредоносных программ для ЭВМ
- О нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети
- О преступлениях в сфере компьютерной информации
- Об ответственности за преступления в сфере компьютерной информации

Вопрос 68

ФЕДЕРАЛЬНЫЙ ЗАКОН «ОБ ИНФОРМАЦИИ, ИНФОРМАТИЗАЦИИ И ЗАЩИТЕ ИНФОРМАЦИИ» НАПРАВЛЕН НА:

- Регулирование взаимоотношений в информационной сфере совместно с гражданским кодексом РФ
- Регулирование взаимоотношений в гражданском обществе РФ
- Регулирование требований к работникам служб, работающих с информаций
- Формирование необходимых норм и правил работы с информацией
- Формирование необходимых норм и правил, связанных с защитой детей от информации

Вопрос 69

ХИЩЕНИЕ ИНФОРМАЦИИ – ЭТО…

- Несанкционированное копирование информации
- Утрата информации
- Блокирование информации
- Искажение информации
- Продажа информации

Вопрос 70

ВЛАДЕЛЬЦЕМ ИНФОРМАЦИИ ПЕРВОЙ КАТЕГОРИИ ЯВЛЯЕТСЯ…

- Государство
- Коммерческая организация
- Муниципальное учреждение
- Любой гражданин
- Группа лиц, имеющих общее дело

Вопрос 71

ВЛАДЕЛЬЦЕМ ИНФОРМАЦИИ ВТОРОЙ КАТЕГОРИИ ЯВЛЯЕТСЯ…

- Простые люди
- Государство
- Коммерческая организация
- Муниципальное учреждение
- Некоммерческая организация

Вопрос 72

ВЛАДЕЛЬЦЕМ ИНФОРМАЦИИ ТРЕТЬЕЙ КАТЕГОРИИ ЯВЛЯЕТСЯ…

- Люди
- Государство
- Муниципальное учреждение
- Учреждение
- Некоммерческая организация

Вопрос 73

ИНФОРМАЦИЕЙ, СОСТАВЛЯЮЩЕЙ ГОСУДАРСТВЕННУЮ ТАЙНУ, ВЛАДЕЮТ:

- Государство
- Только образовательные учреждения
- Только президиум Верховного Совета РФ
- Граждане Российской Федерации
- Только министерство здравоохранения

Вопрос 74

ИНФОРМАЦИЕЙ, СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ, ВЛАДЕЮТ:

- Государство
- Различные учреждения
- Государственная Дума
- Граждане Российской Федерации
- Медико-социальные организации

Вопрос 75

ПЕРСОНАЛЬНЫМИ ДАННЫМИ ВЛАДЕЮТ:

- Государство
- Различные учреждения
- Государственная Дума
- Жители Российской Федерации
- Медико-социальные организации

Вопрос 76

ДОСТУП К ИНФОРМАЦИИ – ЭТО:

- Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя
- Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц
- Действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц
- Информация, переданная или полученная пользователем информационно-телекоммуникационной сети
- Возможность получения информации и ее использования

Вопрос 77

ДОКУМЕНТИРОВАННАЯ ИНФОРМАЦИЯ, ДОСТУП К КОТОРОЙ ОГРАНИЧИВАЕТСЯ В СООТВЕТСТВИИ С ЗАКОНОДАТЕЛЬСТВОМ РОССИЙСКОЙ ФЕДЕРАЦИИ ЭТО:

- Конфиденциальная информация
- Документы офера и договоров
- Факс
- Личный дневник
- Законы РФ

Вопрос 78

ПЛАСТИКОВАЯ КАРТОЧКА, СОДЕРЖАЩАЯ ЧИП ДЛЯ КРИПТОГРАФИЧЕСКИХ ВЫЧИСЛЕНИЙ И ВСТРОЕННУЮ ЗАЩИЩЕННУЮ ПАМЯТЬ ДЛЯ ХРАНЕНИЯ ИНФОРМАЦИИ:

- Токен
- Password
- Пароль
- Login
- Смарт-карта

Вопрос 79

УСТРОЙСТВО ДЛЯ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ, ПРЕДСТАВЛЯЮЩЕЕ СОБОЙ МОБИЛЬНОЕ ПЕРСОНАЛЬНОЕ УСТРОЙСТВО, НАПОМИНАЮЩИЕ МАЛЕНЬКИЙ ПЕЙДЖЕР, НЕ ПОДСОЕДИНЯЕМЫЕ К КОМПЬЮТЕРУ И ИМЕЮЩИЕ СОБСТВЕННЫЙ ИСТОЧНИК ПИТАНИЯ:

- Токен
- Автономный токен
- USB-токен
- Устройство iButton
- Смарт-карта

Вопрос 80

ДОСТУП ПОЛЬЗОВАТЕЛЯ К ИНФОРМАЦИОННЫМ РЕСУРСАМ КОМПЬЮТЕРА И / ИЛИ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ПРЕДПРИЯТИЯ ДОЛЖЕН РАЗРЕШАТЬСЯ ТОЛЬКО ПОСЛЕ:

- Включения компьютера
- Идентификации по логину и паролю
- Запроса паспортных данных
- Запроса доменного имени
- Запроса ФИО

Вопрос 81

АППАРАТНЫЕ МОДУЛИ ДОВЕРЕННОЙ ЗАГРУЗКИ «АККОРД - АМДЗ» ПРЕДСТАВЛЯЮТ СОБОЙ…

- Аппаратный контролер
- Электронный замок
- Система контроля
- Сетевой адаптер
- Копировальный аппарат

Вопрос 82

ЭЛЕКТРОННЫЕ ЗАМКИ «СОБОЛЬ» ПРЕДНАЗНАЧЕНЫ ДЛЯ …

- Обеспечения доверенной загрузки компьютера и контроля целостности файлов в системах
- Сканирования отпечатков пальцев
- Проверки скорости и загрузки файлов
- Общего контроля
- Идентификации пользователя

Вопрос 83

Для защиты от злоумышленников необходимо использовать:

- Системное программное обеспечение
- Прикладное программное обеспечение
- Антивирусные программы
- Компьютерные игры
- Музыку, видеофильмы

Вопрос 84

ФЕДЕРАЛЬНЫЙ ЗАКОН "ОБ ИНФОРМАЦИИ, ИНФОРМАТИЗАЦИИ И ЗАЩИТЕ ИНФОРМАЦИИ" ДАЕТ ОПРЕДЕЛЕНИЕ ИНФОРМАЦИИ:

- Текст книги или письма
- Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления
- Сведения о явлениях и процессах
- Факты и идеи в формализованном виде
- Шифрованный текст, текст на неизвестном языке

Вопрос 85

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЕСТЬ ОБЕСПЕЧЕНИЕ…

- Независимости информации
- Изменения информации
- Копирования информации
- Сохранности информации
- Преобразования информации

Максимальная сумма баллов, набираемая студентом по дисциплине «Информационная безопасность» равна 100.

Оценка в баллах	Оценка по шкале	Обоснование	Уровень сформированности компетенций
Более 80	«Отлично»	Содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному	***Высокий уровень***
66-80	«Хорошо»	Содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками	***Продвинутый уровень***

50-65	«Удовлетворительно»	Содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий, возможно, содержат ошибки	***Пороговый уровень***
Менее 50	«Неудовлетворительно»	Содержание курса не освоено, необходимые практические навыки работы не сформированы, выполненные учебные задания содержат грубые ошибки	Компетенции не сформированы

МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«АРКТИЧЕСКИЙ ГОСУДАРСТВЕННЫЙ АГРОТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО Арктический ГАТУ)
Колледж технологий и управления

Комплект
контрольно-оценочных средств
для проведения тестового контроля

ОП.13 Информационная безопасность
09.02.07 Информационные системы и программирование

Якутск – 2024 г.

Тест ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

1. Под информационной безопасностью понимается…
А) **защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре.**
Б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия
В) нет правильного ответа

2. Защита информации – это..
А) **комплекс мероприятий, направленных на обеспечение информационной безопасности.**
Б) процесс разработки структуры базы данных в соответствии с требованиями пользователей
В) небольшая программа для выполнения определенной задачи

3. От чего зависит информационная безопасность?
А) **от компьютеров**
Б) от поддерживающей инфраструктуры
В) от информации

4. Основные составляющие информационной безопасности:
А) целостность
Б) достоверность
В) конфиденциальность

5. Доступность – это…
А) **возможность за приемлемое время получить требуемую информационную услугу.**
Б) логическая независимость
В) нет правильного ответа

6. Целостность – это..
А) **целостность информации**
Б) непротиворечивость информации
В) защищенность от разрушения

7. Конфиденциальность – это..
А) **защита от несанкционированного доступа к информации**
Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
В) описание процедур

8. Для чего создаются информационные системы?
А) **получения определенных информационных услуг**
Б) обработки информации
В) все ответы правильные

9. Целостность можно подразделить:
А) **статическую**
Б) динамичную
В) структурную

10. Где применяются средства контроля динамической целостности?
А) **анализе потока финансовых сообщений**
Б) обработке данных
В) **при выявлении кражи, дублирования отдельных сообщений**

11. Какие трудности возникают в информационных системах при конфиденциальности?

А) сведения о технических каналах утечки информации являются закрытыми
Б) на пути пользовательской криптографии стоят многочисленные технические проблемы
В) **все ответы правильные**

12. Угроза – это…
А) **потенциальная возможность определенным образом нарушить информационную безопасность**
Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа

13. Атака – это…
А) **попытка реализации угрозы**
Б) потенциальная возможность определенным образом нарушить информационную безопасность
В) программы, предназначенные для поиска необходимых программ.

14. Источник угрозы – это..
А) **потенциальный злоумышленник**
Б) злоумышленник
В) нет правильного ответа

15. Окно опасности – это…
А) **промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется.**
Б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области
В) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере

16. Какие события должны произойти за время существования окна опасности?
А) **должно стать известно о средствах использования пробелов в защите.**
Б) должны быть выпущены соответствующие заплаты.
В) заплаты должны быть установлены в защищаемой И.С.

17. Угрозы можно классифицировать по нескольким критериям:
А) **по спектру И.Б.**
Б) по способу осуществления
В) по компонентам И.С.

18. По каким компонентам классифицируется угрозы доступности:
А) **отказ пользователей**
Б) отказ поддерживающей инфраструктуры
В) ошибка в программе

19. Основными источниками внутренних отказов являются:
А) отступление от установленных правил эксплуатации
Б) разрушение данных
В) **все ответы правильные**

20. Основными источниками внутренних отказов являются:
А) **ошибки при конфигурировании системы**
Б) отказы программного или аппаратного обеспечения
В) выход системы из штатного режима эксплуатации

21. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:
А) **невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности**
Б) обрабатывать большой объем программной информации
В) нет правильного ответа

22. Какие существуют грани вредоносного П.О.?
А) **вредоносная функция**
Б) внешнее представление
В) способ распространения

23. По механизму распространения П.О. различают:
А) вирусы
Б) черви
В) **все ответы правильные**

24. Вирус – это…
А) **код обладающий способностью к распространению путем внедрения в другие программы**
Б) способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов
В) небольшая программа для выполнения определенной задачи

25. Черви – это…
А) **код способный самостоятельно, то есть без внедрения в другие программы вызывать распространения своих копий по И.С. и их выполнения**
Б) код обладающий способностью к распространению путем внедрения в другие программы
В) программа действий над объектом или его свойствами

26. Конфиденциальную информацию можно разделить:
А**) предметную**
Б) служебную
В) глобальную

27. Природа происхождения угроз:
А) **случайные**
Б) преднамеренные
В) природные

28. Предпосылки появления угроз:
А) **объективные**
Б) субъективные
В) преднамеренные

29. К какому виду угроз относится присвоение чужого права?
А) **нарушение права собственности**
Б) нарушение содержания
В) внешняя среда

30. Отказ, ошибки, сбой – это:
А) **случайные угрозы**
Б) преднамеренные угрозы
В) природные угрозы

31. Отказ - это…
А) **нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций**
Б) некоторая последовательность действий, необходимых для выполнения конкретного задания
В) структура, определяющая последовательность выполнения и взаимосвязи процессов

32. Ошибка – это…
А) **неправильное выполнение элементом одной или нескольких функций происходящее в следствии специфического состояния**
Б) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций

В) негативное воздействие на программу

33. Сбой – это…
А) **такое нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент**
Б) неправильное выполнение элементом одной или нескольких функций происходящее в следствие специфического состояния
В) объект-метод

34. Побочное влияние – это…
А) **негативное воздействие на систему в целом или отдельные элементы**
Б) нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
В) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций

35. СЗИ (система защиты информации) делится:
А) **ресурсы автоматизированных систем**
Б) организационно-правовое обеспечение
В) человеческий компонент

36. Что относится к человеческому компоненту СЗИ?
А) **системные порты**
Б) администрация
В) программное обеспечение

37. Что относится к ресурсам А.С. СЗИ?
А) лингвистическое обеспечение
Б) техническое обеспечение
В) **все ответы правильные**

38. По уровню обеспеченной защиты все системы делят:
А) **сильной защиты**
Б) особой защиты
В) слабой защиты

39. По активности реагирования СЗИ системы делят:
А) **пассивные**
Б) активные
В) полупассивные

40. Правовое обеспечение безопасности информации – это…
А) **совокупность законодательных актов, нормативно-правовых документов, руководств, требований, которые обязательны в системе защиты информации**
Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
В) нет правильного ответа

41. Правовое обеспечение безопасности информации делится:
А) международно-правовые нормы
Б) национально-правовые нормы
В) **все ответы правильные**

42. Информацию с ограниченным доступом делят:
А) **государственную тайну**
Б) конфиденциальную информацию
В) достоверную информацию

43. Что относится к государственной тайне?
А) **сведения, защищаемые государством в области военной, экономической … деятельности**
Б) документированная информация
В) нет правильного ответа

44. Вредоносная программа - это…
А) **программа, специально разработанная для нарушения нормального функционирования систем**
Б) упорядочение абстракций, расположение их по уровням
В) процесс разделения элементов абстракции, которые образуют ее структуру и поведение

45. Основополагающие документы для обеспечения безопасности внутри организации:
А) **трудовой договор сотрудников**
Б) должностные обязанности руководителей
В) коллективный договор

46. К организационно - административному обеспечению информации относится:
А) **взаимоотношения исполнителей**
Б) подбор персонала
В) регламентация производственной деятельности

47. Что относится к организационным мероприятиям:
А) **хранение документов**
Б) проведение тестирования средств защиты информации
В) **пропускной режим**

48. Какие средства используется на инженерных и технических мероприятиях в защите информации:
А) **аппаратные**
Б) криптографические
В) физические

49. Программные средства – это…
А) **специальные программы и системы защиты информации в информационных системах различного назначения**
Б) структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач на протяжении всего жизненного цикла
В) модель знаний в форме графа в основе таких моделей лежит идея о том, что любое выражение из значений можно представить в виде совокупности объектов и связи между ними

50. Криптографические средства – это…
А) **средства специальные математические и алгоритмические средства защиты информации, передаваемые по сетям связи, хранимой и обрабатываемой на компьютерах с использованием методов шифрования**
Б) специальные программы и системы защиты информации в информационных системах различного назначения
В) механизм, позволяющий получить новый класс на основе существующего

Тест №1

Инструкция: выберите один правильный ответ

1. В каком году в России появились первые преступления с использованием компьютерной техники (были похищены 125,5 тыс. долларов США во Внешэкономбанке)?
1. 1988;
2. 1991;
3. 1994;
4. 1997;
5. 2002.

2. Сколько выделено основных составляющих национальных интересов Российской Федерации в информационной сфере?

1. 2;
2. 3;
3. 4;
4. 5;
5. 6.

3. Активный перехват информации это перехват, который:
1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
3. неправомерно использует технологические отходы информационного процесса;
4. осуществляется путем использования оптической техники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

4. Обеспечение национальной безопасности на государственном уровне определяется следующей целью:
1. надежная защита личной и имущественной безопасности;
2. обеспечение научно обоснованного и гарантированного государством минимума материальных и экологических условий;
3. преодоление конфронтации в обществе, достижение национального согласия;
4. обеспечение суверенитета и территориальной целостности России.

5. К правовым методам защиты информации относится:
1. разработка нормативно правовых актов, регламентирующих отношения в информационной сфере;
2. создание и совершенствование системы обеспечения ИБ РФ;
3. разработка, использование и совершенствование средств защиты процессов и программ;
4. разработка программ обеспечения ИБ РФ и определение порядка их финансирования;
5. формирование системы мониторинга показателей и характеристик ИБ РФ.

6. В стандарте «Оранжевая книга» фундаментальное требование, которое относится к группе Подотчетность:
1. управляющие доступом метки должны быть связаны с объектами;
2. необходимо иметь явную и хорошо определенную систему обеспечения безопасности;
3. индивидуальные субъекты должны идентифицироваться;
4. вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований;
5. гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений.

7. К источникам защищаемой информации относится:
1. электрические поля;
2. магнитные поля;
3. электромагнитные поля;
4. черновики и отходы производства;
5. элементарные частицы;
6. акустические колебания.

8. Информация, использование которой без согласия субъекта может нанести вред его чести, достоинству, деловой репутации:
1. профессиональная тайна;
2. государственная тайна;
3. персональные данные;
4. коммерческая тайна;

5. служебная тайна.

9. В руководящем документе ФСТЭК системы, в которых работает один пользователь, допущенный ко всей обрабатываемой информации уровня государственной тайны, размещенной на носителях одного уровня конфиденциальности – относятся к группе:
1. 1А;
2. 1Г;
3. 2А;
4. 3А;
5. 3Б.

10. Защита информации от несанкционированного воздействия это деятельность по предотвращению:
1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
2. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
3. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
5. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

ТЕСТ №2

Инструкция: выберите один правильный ответ

1. Какой процент утраты информации от действий собственных сотрудников? 1. 5;
2. 10;
3. 15;
4. 60;
5. 80.

2. Защита информации это:
1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
5. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неѐ.

3. Пассивный перехват информации это перехват, который:
1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
3. неправомерно использует технологические отходы информационного процесса;
4. осуществляется путем использования оптической техники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

2. Обеспечение национальной безопасности на государственном уровне определяется следующей целью:
1. надежная защита личной и имущественной безопасности;
2. обеспечение научно обоснованного и гарантированного государством минимума материальных и экологических условий;
3. преодоление конфронтации в обществе, достижение национального согласия;
4. обеспечение социально-политической и экономической стабильности страны;
5. обеспечение признанных международным правом интересов граждан России, проживающих в зарубежных странах.

5. К правовым методам защиты информации относится:
1. создание и совершенствование системы обеспечения ИБ РФ;
2. разработка, использование и совершенствование средств защиты процессов и программ;
3. внесение изменений и дополнений в законодательство РФ, регулирующие отношения в области обеспечения ИБ;
4. разработка программ обеспечения ИБ РФ и определение порядка их финансирования;
5. формирование системы мониторинга показателей и характеристик ИБ РФ.

6. В стандарте США «Оранжевой книге» фундаментальное требование, которое относится к группе Подотчетность:
1. управляющие доступом метки должны быть связаны с объектами;
2. необходимо иметь явную и хорошо определенную систему обеспечения безопасности;
3. гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений; 4. вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований;
5. контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность.

7. К источникам защищаемой информации относится:
1. электрические поля;
2. сырье;
3. магнитные поля;
4. электромагнитные поля;
5. элементарные частицы;
6. акустические колебания.

8. Естественные угрозы безопасности информации вызваны:
1. деятельностью человека;
2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
3. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
4. корыстными устремлениями злоумышленников;
5. ошибками при действиях персонала.

9. В руководящем документе ФСТЭК системы, в которых работает один пользователь, допущенный ко всей обрабатываемой информации уровня не относящейся к государственной тайне, размещенной на носителях одного уровня конфиденциальности – относятся к группе:
1. 1А;
2. 1Г;
3. 2А;
4. 3А;
5. 3Б.

10. Защита информации от непреднамеренного воздействия это деятельность по предотвращению:
1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
2. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
3. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
5. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

Тест №3

Инструкция: выберите один правильный ответ

1. Какой общий ущерб по данным Института Компьютерной Безопасности нанесли компьютерные вирусы за последние 5 лет, (млрд. долл. США)?
1. 4;
2. 34;
3. 54;
4. 74;
5. 94.

2. Информационные процессы это:
1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
5. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неѐ.

3. Аудиоперехват перехват информации это перехват, который:
1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
3. неправомерно использует технологические отходы информационного процесса;
4. осуществляется путем использования оптической техники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

4. Обеспечение национальной безопасности на государственном уровне определяется следующей целью:
1. защита и обеспечение законных прав, свобод и интересов граждан;
2. надежная защита личной и имущественной безопасности;
3. обеспечение научно обоснованного и гарантированного государством минимума материальных и экологических условий;
4. преодоление конфронтации в обществе, достижение национального согласия;
5. обеспечение признанных международным правом интересов граждан России, проживающих в зарубежных странах.

5. К правовым методам защиты информации относится:

1. создание и совершенствование системы обеспечения ИБ РФ;
2. разработка, использование и совершенствование средств защиты процессов и программ;
3. разработка программ обеспечения ИБ РФ и определение порядка их финансирования;
4. законодательное разграничение полномочий в области ИБ РФ;
5. формирование системы мониторинга показателей и характеристик ИБ РФ.

6. В стандарте «Оранжевая книга» фундаментальное требование, которое относится к группе Гарантии:
1. управляющие доступом метки должны быть связаны с объектами;
2. необходимо иметь явную и хорошо определенную систему обеспечения безопасности;
3. индивидуальные субъекты должны идентифицироваться;
4. вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований;
5. контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность.

7. К носителям защищаемой информации относится:
1. люди
2. сырье;
3. черновики и отходы производства;
4. документы;
5. акустические колебания.

8. Искусственные угрозы безопасности информации вызваны:
1. деятельностью человека;
2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
3. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
4. корыстными устремлениями злоумышленников;
5. ошибками при действиях персонала.

9. В руководящем документе ФСТЭК системы, в которых работает несколько пользователей, которые имеют одинаковые права доступа ко всей информации уровня государственной тайны, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности – относятся к группе:
1. 3А;
2. 2А;
3. 1А;
4. 3Б;
5. 1Б.

10. Защита информации от разглашения это деятельность по предотвращению:
1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
2. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
3. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа; 5. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

Тест №4

Инструкция: выберите один правильный ответ

1. По данным журнала «Security Magazine», средний размер ущерба от компьютерного мошенничества составляет (долл. США):
1. 500 000;
2. 1 000 000;
3. 1 500 000;
4. 2 000 000;
5. 2 500 000.

2. Шифрование информации это:
1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
5. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неѐ.

3. Просмотр мусора это перехват информации, который:
1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
3. неправомерно использует технологические отходы информационного процесса;
4. осуществляется путем использования оптической техники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

4. Обеспечение национальной безопасности на государственном уровне определяется следующей целью:
1. надежная защита личной и имущественной безопасности;
2. совершенствование федеративного государственного устройства;
3. обеспечение научно обоснованного и гарантированного государством минимума материальных и экологических условий;
4. преодоление конфронтации в обществе, достижение национального согласия; 5.обеспечение признанных международным правом интересов граждан России, проживающих в зарубежных странах.

5. К правовым методам защиты информации относится:
1. создание и совершенствование системы обеспечения ИБ РФ;
2. разработка, использование и совершенствование средств защиты процессов и программ;
3. разработка программ обеспечения ИБ РФ и определение порядка их финансирования;
4. формирование системы мониторинга показателей и характеристик ИБ РФ;
5. уточнение статуса иностранных информационных агенств, СМИ и журналистов.

6. В стандарте «Оранжевая книга» фундаментальное требование, которое относится к группе Гарантии:
1. управляющие доступом метки должны быть связаны с объектами;
2. защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений; 3. индивидуальные субъекты должны идентифицироваться;
4. необходимо иметь явную и хорошо определенную систему обеспечения безопасности;
5. контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность.

7. К носителям защищаемой информации относится:
1. элементарные частицы;

2. люди;
3. сырье;
4. черновики и отходы производства;
5. документы.

8. К основным непреднамеренным искусственным угрозам АСОИ относится:
1. физическое разрушение системы путем взрыва, поджога и т.п.;
2. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
5. неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.

9.В руководящем документе ФСТЭК системы, в которых работает несколько пользователей, которые имеют одинаковые права доступа ко всей информации не относящиеся к уровню государственной тайны, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности – относятся к группе:
1. 2Б;
2. 2А;
3. 1А;
4. 3Б;
5. 1Б.

10. Защита информации от несанкционированного доступа это деятельность по предотвращению:
1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
2. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
3. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
5. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

Тест №5

Инструкция: выберите один правильный ответ

1.По данным Главного информационного центра МВД России количество компьютерных преступлений ежегодно увеличивается в (раза):
1. 2;
2. 2,5;
3. 3;
4. 3,5;
5. 4.

2.Доступ к информации это:
1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
2. преобразование информации, в результате которого содержание информации становится

непонятным для субъекта, не имеющего доступа;
3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
5. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неѐ.

3. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:
1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

4. Обеспечение национальной безопасности на государственном уровне определяется следующей целью:
1. надежная защита личной и имущественной безопасности;
2. обеспечение научно обоснованного и гарантированного государством минимума материальных и экологических условий;
3. повышение эффективности защиты конституционного строя, правопорядка, борьбы с орг. преступностью и коррупцией;
4. преодоление конфронтации в обществе, достижение национального согласия;
5. обеспечение признанных международным правом интересов граждан России, проживающих в зарубежных странах.

5. К организационно-техническим методам защиты информации относится:
1. создание и совершенствование системы обеспечения ИБ РФ;
2. разработка программ обеспечения ИБ РФ и определение порядка их финансирования; 3. формирование системы мониторинга показателей и характеристик ИБ РФ;
4. уточнение статуса иностранных информационных агентств, СМИ и журналистов.

6. В международном стандарте «Оранжевая книга» минимальная защита это группа:
1. A;
2. B;
3. C;
4. D;
5. E.

7. К носителям защищаемой информации относится:
1. люди;
2. электрическое поле;
3. сырье;
4. черновики и отходы производства;
5. документы.

8. К основным непреднамеренным искусственным угрозам АСОИ относится:
1. физическое разрушение системы путем взрыва, поджога и т.п.;
2. неправомерное отключение оборудования или изменение режимов работы устройств и программ;
3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
5. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

9. В руководящем документе ФСТЭК многопользовательские системы, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности до грифа «Особо важно» включительно, причем различные пользователи имеют различные права на доступ к информации – относятся к группе:
1. 1Б;
2. 2Б;
3. 3А;
4. 1А;
5. 1В.

10. По характеру воздействия удаленные атаки делятся на:
1. условные и безусловные;
2. атаки с обратной связью и без обратной связи;
3. внутрисегментные и межсегментные;
4. пассивные и активные;
5. атаки, которые могут реализовываться на всех семи уровнях – физическом, канальном, сетевом, транспортном, сеансовом, представительном и прикладном.

Тест №6

Инструкция: выберите один правильный ответ

1. По данным Главного информационного центра МВД России ежегодный размер материального ущерба от компьютерных преступлений составляет около (млн. рублей):
1. 6;
2. 60;
3. 160;
4. 600;
5. 1600.

2. Субъект доступа к информации это:
1.физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;
2.субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации; 3. субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;
4. субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами;
5. участник правоотношений в информационных процессах.

3. Перехват, который осуществляется путем использования оптической техники, называется: 1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

4. Обеспечение национальной безопасности на уровне гражданского общества определяется следующей целью:
1. надежная защита личной и имущественной безопасности;
2. обеспечение научно обоснованного и гарантированного государством минимума материальных и экологических условий;
3. повышение эффективности защиты конституционного строя, правопорядка, борьбы с орг. преступностью и коррупцией;

4. преодоление конфронтации в обществе, достижение национального согласия.

5. К организационно-техническим методам защиты информации относится:
1. разработка программ обеспечения ИБ РФ и определение порядка их финансирования;
2. формирование системы мониторинга показателей и характеристик ИБ РФ;
3. уточнение статуса иностранных информационных агентств, СМИ и журналистов;
4. усиление правоприменительной деятельности федеральных органов исполнительной власти в информационной сфере.

6. В международном стандарте «Оранжевая книга» индивидуальная защита это группа:
1. A;
2. B;
3. C;
4. D;
5. E.

7. К носителям защищаемой информации относится:
1. люди;
2. сырье;
3. черновики и отходы производства;
4. магнитное поле;
5. документы.

8. К основным непреднамеренным искусственным угрозам АСОИ относится:
1. физическое разрушение системы путем взрыва, поджога и т.п.;
2. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
4. неумышленная порча носителей информации;
5. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

9. В руководящем документе ФСТЭК многопользовательские системы, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности до грифа «Совершенно секретно» включительно, причем различные пользователи имеют различные права на доступ к информации – относятся к группе:
1. 1Б;
2. 2Б;
3. 3А;
4. 1А;
5. 1В.

10. По цели воздействия удаленные атаки делятся на:
1. условные и безусловные;
2. атаки с обратной связью и без обратной связи;
3. внутрисегментные и межсегментные;
4. пассивные и активные;
5. атаки в зависимости от нарушения конфиденциальности, целостности и доступности.

Тест №7

Инструкция: выберите один правильный ответ

1. По данным Главного информационного центра МВД России средний ущерб, причиняемый потерпевшему от 1 компьютерного преступления, равен (млн. рублей):

1. 7;
2. 1,7;
3. 2,7;
4. 3,7;
5. 4,7.

2. Носитель информации это:

1. физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;
2. субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации; 3. субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;
4. субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами;
5. участник правоотношений в информационных процессах.

3. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:
1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

4. Обеспечение национальной безопасности на уровне гражданского общества определяется следующей целью:
1. надежная защита личной и имущественной безопасности;
2. обеспечение научно обоснованного и гарантированного государством минимума материальных и экологических условий;
3. обеспечение признанных международным правом интересов граждан России, проживающих в зарубежных странах;
4. повышение эффективности защиты конституционного строя, правопорядка, борьбы с орг. преступностью и коррупцией;

5. К организационно-техническим методам защиты информации относится:
1. разработка программ обеспечения ИБ РФ и определение порядка их финансирования;
2. формирование системы мониторинга показателей и характеристик ИБ РФ;
3. уточнение статуса иностранных информационных агентств, СМИ и журналистов;
4. внесение изменений и дополнений в законодательство РФ, регулирующие отношения в области обеспечения ИБ;
5. формирование системы мониторинга показателей и характеристик ИБ РФ.

6. В международном стандарте «Оранжевая книга» мандатная защита это группа:
1. A;
2. B;
3. C;
4. D;
5. E.

7. Защищаемые государством сведения, распространение которых может нанести ущерб РФ, это:
1. профессиональная тайна;
2. государственная тайна;

3. персональные данные;
4. коммерческая тайна;
5. служебная тайна.

8. К основным непреднамеренным искусственным угрозам АСОИ относится:
1.запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы;
2.чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
3.изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
4.физическое разрушение системы путем взрыва, поджога и т.п.;
5.перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

9. В руководящем документе ФСТЭК многопользовательские системы, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности до грифа «Секретно» включительно, причем различные пользователи имеют различные права на доступ к информации – относятся к группе:
1. 1Б;
2. 2Б;
3. 3А;
4. 1А;
5. 1В.

10. По условию начала осуществления воздействия удаленные атаки делятся на:
1. условные и безусловные;
2. атаки с обратной связью и без обратной связи;
3. внутрисегментные и межсегментные;
4. пассивные и активные;
5. атаки в зависимости от нарушения конфиденциальности, целостности и доступности.

Тест №8

Инструкция: выберите один правильный ответ
1. Сколько процентов электронных писем являются
Спамом? 1. 10;
2. 30;
3. 50;
4. 70;
5. 90.

2. Собственник информации это:
1. физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;
2. субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;
3. субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;
4. субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами;
5. участник правоотношений в информационных процессах.

3. Перехват, который осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера называется:
1. активный перехват;
2. пассивный перехват;

3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

4. Обеспечение национальной безопасности на уровне гражданского общества определяется следующей целью:
1. надежная защита личной и имущественной безопасности;
2. ускорение процессов формирования институтов самоорганизации гражданского общества;
3. обеспечение научно обоснованного и гарантированного государством минимума материальных и экологических условий;
4. повышение эффективности защиты конституционного строя, правопорядка, борьбы с орг. преступностью и коррупцией;
5. обеспечение суверенитета и территориальной целостности России.

5. К экономическим методам защиты информации относится:
1. разработка программ обеспечения ИБ РФ и определение порядка их финансирования;
2. уточнение статуса иностранных информационных агентств, СМИ и журналистов;
3. внесение изменений и дополнений в законодательство РФ, регулирующие отношения в области обеспечения ИБ;
4. формирование системы мониторинга показателей и характеристик ИБ РФ.

6. В международном стандарте «Оранжевая книга» верифицированная защита это группа: 1. A;
2. B;
3. C;
4. D;
5. E.

7. Информация представляющая секрет производства(ноу-хау), это:
1. профессиональная тайна;
2. государственная тайна;
3. персональные данные;
4. коммерческая тайна;
5. служебная тайна.

8. К основным непреднамеренным искусственным угрозам АСОИ относится:
1. физическое разрушение системы путем взрыва, поджога и т.п.;
2. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
4. нелегальное внедрение и использование неучтенных программ игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения служебных обязанностей;
5. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

9. В руководящем документе ФСТЭК многопользовательские системы, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности в том числе Персональные данные, причем различные пользователи имеют различные права на доступ к информации – относятся к группе:
1. 1Б;
2. 1Г;
3. 3А;
4. 1А;
5. 1В.

10. По наличию обратной связи с атакуемым объектом удаленные атаки делятся на:
1. условные и безусловные;
2. атаки с обратной связью и без обратной связи;
3. внутрисегментные и межсегментные;
4. пассивные и активные;
5. атаки в зависимости от нарушения конфиденциальности, целостности и доступности.

Критерии оценивания:

Оценки "отлично" заслуживает студент, обнаруживший всестороннее, систематическое и глубокое знание учебно-программного материала, умение свободно выполнять задания, предусмотренные программой, усвоивший основную и знакомый с дополнительной литературой, рекомендованной программой. Как правило, оценка "отлично" выставляется студентам, усвоившим взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявившим творческие способности в понимании, изложении и использовании учебно-программного материала.

Оценки "хорошо" заслуживает студент обнаруживший полное знание учебно-программного материала, успешно выполняющий предусмотренные в программе задания, усвоивший основную литературу, рекомендованную в программе. Как правило, оценка "хорошо" выставляется студентам, показавшим систематический характер знаний по дисциплине и способным к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.

Оценки "удовлетворительно" заслуживает студент, обнаруживший знания основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по специальности, справляющийся с выполнением заданий, предусмотренных программой, знакомый с основной литературой, рекомендованной программой. Как правило, оценка "удовлетворительно" выставляется студентам, допустившим погрешности в ответе на экзамене и при выполнении экзаменационных заданий, но обладающим необходимыми знаниями для их устранения под руководством преподавателя.

Оценка "неудовлетворительно" выставляется студенту, обнаружившему пробелы в знаниях основного учебно-программного материала, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий. Как правило, оценка "неудовлетворительно" ставится студентам, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.

МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«АРКТИЧЕСКИЙ ГОСУДАРСТВЕННЫЙ АГРОТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО Арктический ГАТУ)
Колледж технологий и управления

Комплект
контрольно-оценочных средств
для промежуточной аттестации по результатам освоения дисциплины

ОП.13 Информационная безопасность

09.02.07 Информационные системы и программирование

Якутск – 2024 г.

Примерный перечень теоретических вопросов для зачета:

1. Информационная безопасность человека и общества. Уровни защиты информационных ресурсов. Признаки, свидетельствующие о наличии уязвимых мест в информационной безопасности.
2. Компьютерные преступления. Основные технологии, использующиеся при совершении компьютерных преступлений.
3. Объекты защиты информации. Защита информации ограниченного доступа: гос
4. Основные каналы утечки информации. Защита от утечки информации по техническим каналам.
5. Методы и средства защиты информации. Содержание способов и средств обеспечения безопасности информации.
6. Реализация методов и средств защиты информации.
7. Средства опознания и разграничения доступа к информации.
8. Криптография. Симметричные криптосистемы.
9. Криптография. Асимметричные криптосистемы.
10. Обзор и классификация методов шифрования информации.
11. Электронно-цифровая подпись.
12. Основные алгоритмы шифрования данных: ГОСТ.
13. Правовые средства защиты информации. Защита программных продуктов. Авторское право.
14. Защита данных в автономном компьютере.
15. Защита данных в вычислительных сетях. Разработка сетевых аспектов политики бе
16. Защита данных в вычислительных сетях. Межсетевые экраны. Сканеры.
17. Показатели оценки достоверности (безошибочности) передачи данных в сетях.
18. Методы взлома компьютерных систем: атаки на уровне операционных систем, атаки на уровне программного обеспечения, атаки на уровне систем управления базами данных.
19. Парольная защита операционных систем. Парольные взломщики.
20. Понятие угрозы. Анализ угроз информационной безопасности. Виды «нарушителей».
21. Структуризация методов обеспечения информационной безопасности. Основные методы реализации угроз информационной безопасности.
22. Основные принципы обеспечения информационной безопасности в автоматизированной системе.
23. Причины, виды и каналы утечки информации.
24. Методы построения защищенных автоматизированных систем.
25. Политика безопасности. Основные типы политики безопасности.
26. Политика безопасности. Модели безопасности.

27. Стандарты информационной безопасности.
28. Правовое обеспечение защиты информации. Нормативные документы.
29. Разрушающие программные воздействия: вирусы и закладки. Антивирусные средства.
30. Психологические аспекты информационной безопасности организации.

Примерный перечень практических заданий для зачета:

1. Создание шифрованных пользовательских виртуальных дисков.
2. Анализ программных средств криптографической защиты информации.
3. Анализ программно-аппаратных средств усиленной аутентификации
4. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям
5. Настройка политики безопасности операционной системы.
6. Анализ защищенности изолированной программной среды.
7. Исследование систем идентификации.
8. Обзор средств построения виртуальных частных сетей.
9. Изучение средств межсетевого экранирования
10. Исследование технологий доверенной загрузки операционной системы
11. Методы сокрытия программных закладок.
12. Средства идентификации и аутентификации объектов баз данных, управление доступом
13. Средства контроля целостности информации, организация аудита
14. Типы контроля безопасности: потоковый, контроль вывода, контроль доступа.
15. Использование програмных средств для изолирования действий пользователей