АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОБРАЗОВАТЕЛЬНАЯ
ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
ЦЕНТРОСОЮЗА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ УНИВЕРСИТЕТ КООПЕРАЦИИ»
КАЗАНСКИЙ КООПЕРАТИВНЫЙ ИНСТИТУТ (ФИЛИАЛ)

.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки: 38.03.05 Бизнес-информатика
Направленность (профиль): «Электронный бизнес».
Форма обучения: очная, заочная
Квалификация (степень) выпускника: бакалавр
Срок обучения: очная форма – 4 года, заочная форма - 4 года 6 мес.

Вид учебной работы	Трудоемкость, часы (з.е.)	
	Очная форма	Заочная форма
1. Контактная работа обучающихся с преподавателем:	52(1,44)	10(0,28)
Аудиторные занятия, часов всего, в том числе:	50(1,39)	8(0,22)
• лекции	16(0,44)	2(0,06)
• лабораторные работы	34(0,94)	6(0,17)
Промежуточная аттестация (контактная работа)	2(0,06)	2(0,06)
2. Самостоятельная работа студентов, всего	58(1,61)	127(3,53)
• др. формы самостоятельной работы	58(1,61)	127(3,53)
3. Промежуточная аттестация: экзамен	34(0,94)	7(0,19)
Итого	144(4)	144(4)

Казань 2018

Фахертдинова Д.И. Информационная безопасность: Рабочая программа учебной дисциплины (модуля). – Казань: Казанский кооперативный институт (филиал) Российского университета кооперации, 2018. – 55 с.

Рабочая программа по дисциплине (модулю) «Информационная безопасность» по направлению подготовки 38.03.05 Бизнес-информатика, направленность «Электронный бизнес» составлена Фахертдинова Д.И., к.п.н., доцентом кафедры естественных дисциплин, сервиса и туризма Казанского кооперативного института (филиала) Российского университета кооперации в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки «Бизнес-информатика», утвержденного приказом Министерства образования и науки Российской Федерации от «11» августа 2016 г. № 1002, и учебными планами по направлению подготовки 38.03.05 Бизнес-информатика, направленность (профиль) «Электронный бизнес» (год начала подготовки -2018).

Рабочая программа:

обсуждена и рекомендована к утверждению решением кафедры естественных дисциплин, сервиса и туризма Казанского кооперативного института (филиала) Российского университета кооперации от «10» мая 2018 г., протокол № 3.

одобрена Научно-методическим советом Казанского кооперативного института (филиала) от 23.05.2018, протокол № 5.

утверждена Ученым советом Российского университета кооперации от 30.05.2018, протокол № 7.

СОДЕРЖАНИЕ

1. Цели и задачи освоения дисциплины (модуля)

Цели и задачи изучения дисциплины – ознакомление студентов с основными понятиями и определениями информационной безопасности; источниками, рисками и формами атак на информацию; угрозами, которым подвергается информация; вредоносными программами; защитой от компьютерных вирусов и других вредоносных программ; методами и средствами защиты информации; политикой безопасности компании в области информационной безопасности; стандартами информационной безопасности; криптографическими методами и алгоритмами шифрования информации; алгоритмами аутентификации пользователей; защитой информации в сетях; требованиям к системам защиты информации

2. Место дисциплины (модуля) в структуре основной образовательной программы

Дисциплина относится к базовой части дисциплин блока Б1 «Дисциплины (модули)»

Для изучения учебной дисциплины необходимы следующие знания, умения и владения навыками, формируемые предшествующими дисциплинами:

Теоретические основы информатики (ОПК-3)

3. Перечень планируемых результатов обучения по дисциплине (модулю)

Изучение дисциплины направлено на формирование у обучающихся следующих компетенций:

ОПК-1 - способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

ПК-9 - организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия;

Формируемые компетенции (код компетенции)	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций	Наименование оценочного средства
ОПК-1 ПК-9	Знать основные методы принятия организационно-управленческих решений, основные методики взаимодействия с обществом, коллективом, партнерами в своей профессиональной деятельности;	Доклад

Формируемые компетенции (код компетенции)	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций	Наименование оценочного средства
	Знать современные методы управления информационной безопасности ИТ- инфраструктуры предприятия;	
	Знать специфику создания и развития ИТ-инфраструктуры предприятия	
ОПК-1 ПК-9	Уметь анализировать и выбирать организационно-управленческие решения в своей деятельности, осознавать ответственность за принимаемые решения, добиваться поставленных задач во взаимодействии с обществом, коллективом, партнерами;	Лабораторная работа
	Уметь обосновывать необходимость совершенствования управления информационной безопасностью предприятия, необходимость создания, развития и модернизации ИТ-инфраструктуры предприятия;	
ОПК-1 ПК-9	Владеть навыками выработки организационно-управленческих решений, ответственного их исполнения во взаимодействии с обществом, коллективом, партнерами;	Самостоятельная работа Контрольная работа
	Владеть навыками консультирования клиентов и партнеров по вопросам совершенствования управления информационной безопасностью и бизнес процессов ИТ-инфраструктуры предприятия	

4. Объем дисциплины (модуля) и виды учебной работы

очная форма обучения

Вид учебной деятельности		Часов	
		Всего	По семестрам
			4
1. Контактная работа обучающихся с преподавателем:		52	52
Аудиторные занятия всего, в том числе:		50	50
Лекции		16	16
Лабораторные занятия		34	34
Промежуточная аттестация (контактная работа)		2	2
2. Самостоятельная работа студента всего, в том числе:		58	58
Другие виды самостоятельной работы		58	58
Вид промежуточной аттестации - экзамен		34	34
ИТОГО:	часов	144	144
Общая трудоемкость	зач. ед.	4	4

заочная форма обучения

Вид учебной деятельности	Часов	
	Всего	По курсам
		3
1. Контактная работа обучающихся с преподавателем:	10	10
Аудиторные занятия всего, в том числе:	8	8
Лекции	2	2
Лабораторные занятия	6	6
Промежуточная аттестация (контактная работа)	2	2

Вид учебной деятельности		Часов	
		Всего	По курсам
			3
2. Самостоятельная работа студента всего, в том числе:		127	127
Другие виды самостоятельной работы		127	127
Вид промежуточной аттестации - экзамен		7	7
ИТОГО:	часов	144	144
Общая трудоемкость	зач. ед.	4	4

5. Содержание учебной дисциплины (модуля)

5.1. Содержание разделов, тем дисциплины (модуля)

Тема 1. Основные понятия и положения информационной безопасности

Информация, сообщения, информационные процессы как объекты информационной безопасности. Цели и задачи защиты информации. Классификационная схема понятий в области защиты информации. Концептуальные основы защиты информации. Основные положения государственной политики обеспечения информационной безопасности РФ

Тема 2. Угрозы безопасности информации в информационных системах

Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации. Методы оценки уязвимости информации. Виды утечки информации. Анализ угроз информационной безопасности. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы. Структура теории компьютерной безопасности. Основные уровни защиты информации. Защита машинных носителей информации (МНИ). Защита средств взаимодействия с МНИ. Защита представления информации. Защита содержания информации. Основные виды атак на информационные АС. Классификация основных атак и вредоносных программ.

Тема 3. Методы и средства защиты информации

Классификация методов и средств защиты информации. Правовые методы обеспечения информационной безопасности. Организационно-технические методы обеспечения информационной безопасности. Экономические методы обеспечения информационной безопасности.

Стандарты информационной безопасности, критерии и классы оценки защищенности компьютерных систем и сетей. Основные критерии защищенности информационных автоматизированных систем систем (АС). Классы защищенности АС. Критерии и классы защищенности средств вычислительной техники (СВТ) и АС.

Стандарты по оценке защищенности АС. Стандарт оценки безопасности компьютерных систем TCSEC («Оранжевая книга»). Основные требования к системам защиты в TCSEC. Классы защиты TCSEC. Концепция защиты АС и СВТ по руководящим документам Гостехкомиссии РФ.

Тема 4. Криптографические методы защиты информации

Классификация методов криптографического преобразования информации: шифрование, стеганофрация, кодирование, сжатие. Требования к методам шифрования и их классификация. Криптостойкость шифра как основной показатель его эффективности.

Методы шифрования с симметричным ключом: методы замены, методы перестановки, аналитические методы, аддитивные методы, комбинированные методы. Системы шифрования с открытым ключом. Стандарты шифрования. Перспективы использования криптозащиты информации.

Тема 5. Аппаратные и программные средства защиты компьютерной информации

Основные понятия программно-технического уровня информационной безопасности. Архитектурная безопасность. Современные способы и средства негласного получения информации по различным каналам. Пассивные и активные способы обеспечения информационной безопасности. Современные средства выявления каналов утечки информации

Тема 6. Безопасность компьютерных сетей

Основные аспекты безопасности компьютерных сетей (КС). Атакуемые сетевые компоненты на разных уровнях модели OSI, уязвимости сетевых служб (DNS, Telnet), средств передачи информации. Классификация сетевых атак. Межсетевые экраны. Типы и функции межсетевых экранов: пакетных фильтров, прокси-систем, устройств контроля текущего состояния.

Организация виртуальных корпоративных сетей. Протокол IPSec. Защита данных в WWW.

Классификация компьютерных вирусов. Меры по их профилактике. Методология защиты автоматизированных информационных систем. Антивирусные программы.

5.2. Междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами (модулями)

Дисциплина «Информационная безопасность» формирует ОПК-1, ПК-9 компетенции, необходимые в дальнейшем для формирования компетенций преддипломной практики.

5.3. Разделы, темы дисциплины (модуля) и виды занятий

очная форма обучения

№ п/п	Наименование раздела, темы учебной дисциплины (модуля)	Виды занятий, включая состоятельную работу студентов (в часах)			
		Лекции	Лабораторные занятия	Самостоятельная работа	Всего
1.	Основные понятия и положения информационной безопасности.	2	-	8	10
2.	Угрозы безопасности информации в информационных системах.	2	16	10	28
3.	Методы и средства защиты информации.	2	18	10	30
4.	Криптографические методы защиты информации.	2	-	10	12
5.	Аппаратные и программные средства защиты компьютерной информации.	4	-	10	14
6.	Безопасность компьютерных сетей.	4	-	10	14
	ИТОГО:	**16**	**34**	**58**	**108**

заочная форма обучения

№ п/п	Наименование раздела, темы учебной дисциплины (модуля)	Виды занятий, включая состоятельную работу студентов (в часах)			
		Лекции	Лабораторные занятия	Самостоятельная работа	Всего
1.	Основные понятия и положения информационной безопасности.	1	-	20	21
2.	Угрозы безопасности информации в информационных системах.	-	2	20	22
3.	Методы и средства защиты информации.	1	4	20	25
4.	Криптографические методы защиты информации.	-	-	20	20
5.	Аппаратные и программные средства защиты компьютерной информации.	-	-	20	20
6.	Безопасность компьютерных сетей.	-	-	27	27
	ИТОГО:	**2**	**6**	**127**	**135**

6. Лабораторный практикум

Лабораторные занятия проводятся с целью формирования компетенций обучающихся, закрепления полученных теоретических знаний на лекциях и в процессе самостоятельного изучения обучающимися специальной литературы

очная форма обучения

№ п/п	Наименование раздела, темы учебной дисциплины (модуля)	Тематика лабораторных занятий	Трудоемкость (час.)
1	Угрозы безопасности информации в информационных системах.	Основные виды атак на информационные АС. Классификация основных атак и вредоносных программ.	16

№ п/п	Наименование раздела, темы учебной дисциплины (модуля)	Тематика лабораторных занятий	Трудоемкость (час.)
2	Методы и средства защиты информации.	Стандарт оценки безопасности компьютерных систем TCSEC («Оранжевая книга»). Основные требования к системам защиты в TCSEC. Концепция защиты АС и СВТ по руководящим документам Гостехкомиссии РФ.	18
	Итого		**34**

заочная форма обучения

№ п/п	Наименование раздела, темы учебной дисциплины (модуля)	Тематика лабораторных занятий	Трудоемкость (час.)
1	Угрозы безопасности информации в информационных системах.	Основные виды атак на информационные АС. Классификация основных атак и вредоносных программ.	2
2	Методы и средства защиты информации.	Стандарт оценки безопасности компьютерных систем TCSEC («Оранжевая книга»). Основные требования к системам защиты в TCSEC. Концепция защиты АС и СВТ по руководящим документам Гостехкомиссии РФ.	4
	Итого		**6**

7. Практические занятия (семинары)

Практические занятия не предусмотрены учебными планами.

8. Примерная тематика курсовых проектов (работ)

Курсовые проекты (работы) не предусмотрены учебными планами.

9. Самостоятельная работа студента

Тема 1. Основные понятия и положения информационной безопасности.

Вид самостоятельной работы:

Изучение учебных пособий. Работа с конспектом лекций. Ответы на контрольные вопросы.

Рекомендации: Обратить внимание на ФЗ-149 и ФЗ-152.

Оценочное средство: доклад

Тема 2. Угрозы безопасности информации в информационных системах.

Вид самостоятельной работы:

Изучение учебных пособий. Работа с конспектом лекций. Ответы на контрольные вопросы. Подготовка к лабораторным работам.

Рекомендации: Обратить внимание на виды угроз.

Оценочное средство: лабораторная работа

Тема 3. Методы и средства защиты информации.

Вид самостоятельной работы:

Изучение учебных пособий. Работа с конспектом лекций. Подготовка к лабораторным работам.

Рекомендации: Обратить внимание на все разновидности средств защиты информации.

Оценочное средство: лабораторная работа

Тема 4. Криптографические методы защиты информации.

Вид самостоятельной работы:

Изучение учебных пособий. Работа с конспектом лекций. Подготовка к лабораторным работам.

Рекомендации: Обратить внимание на криптографические методы защиты информации.

Оценочное средство: контрольная работа

Тема 5. Аппаратные и программные средства защиты компьютерной информации.

Вид самостоятельной работы:

Изучение учебных пособий. Работа с конспектом лекций. Подготовка к лабораторным работам.

Рекомендации: Обратить внимание на аппаратные и программные средства защиты компьютерной информации. Их функции и возможности.

Оценочное средство: реферат / опрос

Тема 6. Безопасность компьютерных сетей.

Вид самостоятельной работы:

Изучение учебных пособий. Работа с конспектом лекций. Подготовка к лабораторным работам.

Рекомендации: Обратить внимание на средства обеспечения безопасности компьютерных сетей.

Оценочное средство: лабораторная работа.

10. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Самостоятельная работа студентов предполагает тщательное освоение учебной и научной литературы по изучаемой дисциплине.

При изучении основной рекомендуемой литературы студентам необходимо обратить внимание на выделение основных понятий, их определения, научно-технические основы, узловые положения, представленные в изучаемом тексте.

При самостоятельной работе студентов с дополнительной литературой необходимо выделить аспект изучаемой темы (что в данном материале относится непосредственно к изучаемой теме и основным вопросам).

Дополнительную литературу целесообразно прорабатывать после основной, которая формирует базис для последующего более глубокого изучения темы. Дополнительную литературу следует изучать комплексно, рассматривая разные стороны изучаемого вопроса. Обязательным элементом самостоятельной работы студентов с литературой является ведение необходимых записей: конспекта, выписки, тезисов, планов.

Для самостоятельной работы по дисциплине используется следующее учебно-методическое обеспечение:

а) основная литература

1. Информационная безопасность и защита информации: Учебное пособие / Баранова Е. К., Бабаш А. В. - 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с. - Режим доступа: http://znanium.com/catalog/product/495249

2. Информационная безопасность предприятия: Учебное пособие / Гришина Н.В., - 2-е изд., доп - М.: Форум, НИЦ ИНФРА-М, 2016. - 240 с.- Режим доступа: http://znanium.com/catalog/product/544554

б) дополнительная литература

1. Башлы, П. Н. Информационная безопасность и защита информации : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - Режим доступа: http://znanium.com/catalog/product/405000

11. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

а) основная литература

1. Информационная безопасность и защита информации: Учебное пособие / Баранова Е. К., Бабаш А. В. - 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с. - Режим доступа: http://znanium.com/catalog/product/495249

2. Информационная безопасность предприятия: Учебное пособие / Гришина Н.В., - 2-е изд., доп - М.: Форум, НИЦ ИНФРА-М, 2016. - 240 с.- Режим доступа: http://znanium.com/catalog/product/544554

б) дополнительная литература

1. Башлы, П. Н. Информационная безопасность и защита информации : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - Режим доступа: http://znanium.com/catalog/product/405000

12. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

- https://www.book.ru/ - ЭБС Book.ru

- http://www.iprbookshop.ru - ЭБС IPRbooks
- https://ibooks.ru/ -ЭБС Айбукс.ru/ibooks.ru
- https://rucont.ru/ - ЭБС «Национальный цифровой ресурс «Руконт»
- http://znanium.com/ - ЭБС Znanium.com
- https://dlib.eastview.com/- База данных East View

13. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

1. Desktop School ALNG LicSAPk MVL.
   a. Office ProPlus All Lng Lic/SA Pack MVL Partners in Learning (лицензия на пакет Office Professional Plus)
   b. Windows 8
2. Система тестирования INDIGO.
3. Adobe Acrobat – свободно-распространяемое ПО
4. Интернет-браузеры Google Chrome, Firefox – свободно-распространяемое ПО
5. Консультант + версия проф.- справочная правовая система

Каждый обучающийся в течение всего обучения обеспечивается индивидуальным неограниченным доступом электронно-библиотечной системе и электронной информационно-образовательной среде.

14. Описание материально- технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Образовательный процесс обеспечивается специальными помещениями, которые представляют собой аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещения для самостоятельной работы студентов и помещения для хранения и профилактического обслуживания учебного оборудования.

Специальные помещения соответствуют действующим противопожарным правилам и нормам, укомплектованы специализированной мебелью.

Аудитории лекционного типа, оснащенные проекционным оборудованием и техническими средствами обучения, обеспечивающими представление учебной информации большой аудитории, демонстрационным оборудованием.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, обеспечивающей доступ к сети Интернет и электронной информационно-образовательной среде университета.

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

Дисциплина «Информационная безопасность» состоит из 6 тем и изучается на лекциях, лабораторных занятиях и при самостоятельной работе обучающихся. Обучающийся для полного освоения материала должен не пропускать занятия и активно участвовать в учебном процессе. Кроме того, обучающиеся должны ознакомиться с программой дисциплины и списком основной и дополнительной рекомендуемой литературы.

Основной теоретический материал дается на лекционных занятиях. Лекции включают все темы и основные вопросы теории и практики информационной безопасности. Для максимальной эффективности изучения необходимо постоянно вести конспект лекций, знать рекомендуемую преподавателем основную и дополнительную учебную литературу, позволяющую дополнить знания и лучше подготовиться к практическим занятиям.

Для закрепления теоретического материала, формирования профессиональных компетенций и практических навыков принятия стратегических решений со студентами бакалавриата проводятся лабораторные занятия. В ходе занятий разбираются основные и дополнительные теоретические вопросы информационных систем, решаются практические задачи на разработку и обоснование стратегических решений, проводятся тестирования по результатам изучения тем.

На изучение каждой темы выделено в соответствие с рабочей программой дисциплины количество часов лабораторных занятий, которые проводятся в соответствии с вопросами, рекомендованными к изучению по определенным темам. Обучающиеся должны регулярно готовиться к лабораторным занятиям. При подготовке к занятиям следует руководствоваться конспектом лекций и рекомендованной литературой.

Для эффективного освоения материала дисциплины учебным планом предусмотрена самостоятельная работа, которая должна выполняться в обязательном порядке. Выполнение самостоятельной работы по темам дисциплины, позволяет регулярно проводить самооценку качества усвоения материалов дисциплины и выявлять аспекты, требующие более детального изучения. Задания для самостоятельной работы предложены по каждой из изучаемых тем и должны готовиться индивидуально и к указанному сроку. По необходимости студент бакалавриата может обращаться за консультацией к преподавателю. Выполнение заданий контролируется и оценивается преподавателем.

В случае посещения обучающегося лекций и лабораторных занятий, изучения рекомендованной основной и дополнительной учебной литературы, а также своевременного и самостоятельного выполнения заданий, подготовка к экзамену по дисциплине сводится к дальнейшей систематизации полученных знаний, умений и навыков.

16. Методические рекомендации по организации изучения дисциплины для преподавателей, образовательные технологии

Оценочные средства для контроля успеваемости и результатов освоения дисциплины (модуля):

а) для текущей успеваемости: доклад, лабораторная работа, самостоятельная работа, контрольная работа;

б) для самоконтроля обучающихся: тесты;

в) для промежуточной аттестации: вопросы для экзамена, практические задания

При реализации различных видов учебной работы по дисциплине «Информационная безопасность», оценка возможных последствий и контроль над исполнением» используются следующие образовательные технологии:

1)лекции с использованием методов проблемного изложения материала;

2)обсуждение и защита лабораторных работ

№	Занятие в интерактивной форме	Количество часов по очной форме		Количество часов по заочной форме	
		Лекция	Лаборат.	Лекция	Лаборат.
1.	Угрозы безопасности информации в информационных системах. Вид: Лекция с демонстрацией видеоматериалов (слайды) Лабораторные занятия с применением следующих технологий: - обсуждение и защита лабораторных работ	2	4	-	2
2.	Методы и средства защиты информации. Вид: Лекция с демонстрацией видеоматериалов (слайды) Лабораторные занятия с применением следующих технологий: - обсуждение и защита лабораторных работ	2	4	1	4
	Итого	4	8	1	**6**

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОБРАЗОВАТЕЛЬНАЯ
ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
ЦЕНТРОСОЮЗА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ УНИВЕРСИТЕТ КООПЕРАЦИИ»
КАЗАНСКИЙ КООПЕРАТИВНЫЙ ИНСТИТУТ (ФИЛИАЛ)

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки: 38.03.05 Бизнес-информатика
Направленность: «Электронный бизнес»

1. Паспорт фонда оценочных средств

1. 1. Компетенции, формируемые в процессе изучения дисциплины

Индекс	Формулировка компетенции
ОПК-1	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ПК-9	организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия

1.2. Сведения об иных дисциплинах (преподаваемых, в том числе, на других кафедрах) участвующих в формировании данных компетенций

1.2.1 Компетенция ОПК-1 формируется в процессе изучения дисциплин (прохождения практик):

Базы данных

Вычислительные системы, сети, телекоммуникации

Архитектура электронного предприятия

ИТ-инфраструктура предприятия

Моделирование бизнес-процессов

Управление жизненным циклом информационных систем

Разработка ИТ- сервисов предприятия

Компьютерная графика и дизайн

Учебная практика. Практика по получению первичных профессиональных умений и навыков проектной деятельности, в том числе первичных умений и навыков научно-исследовательской деятельности

1.2.2 Компетенция ПК-9 формируется в процессе изучения дисциплин (прохождения практик):

Коммуникативная культура профессионала

Культура профессионального самообразования

Стратегия управления взаимоотношениями с клиентами (CRM-системы)

Информационный менеджмент

Производственная практика. Практика по получению профессиональных умений и опыта профессиональной деятельности

1.3. Этапы формирования и программа оценивания контролируемой компетенции

№	Код контролируемой компетенции	Контролируемые темы дисциплины	Наименование оценочного средства
1 2	ОПК-1 ПК-9	Тема 1. Основные понятия и положения информационной	Доклад Самостоятельная работа

№	Код контролируемой компетенции	Контролируемые темы дисциплины	Наименование оценочного средства
		безопасности. Тема 2. Угрозы безопасности информации в информационных системах. Тема 3. Методы и средства защиты информации. Тема 4. Криптографические методы защиты информации. Тема 5. Аппаратные и программные средства защиты компьютерной информации. Тема 6. Безопасность компьютерных сетей.	Лабораторная работа Контрольная работа

Процедура оценивания

1. Процедура оценивания результатов освоения программы учебной дисциплины включает в себя оценку уровня сформированности компетенций студента при осуществлении текущего контроля и проведении промежуточной аттестации.
2. Уровень сформированности компетенции (ОПК-1, ПК-9) определяется по качеству выполненной студентом работы и отражается в следующих формулировках: высокий, хороший, достаточный, недостаточный.
3. При выполнении студентами заданий текущего контроля и промежуточной аттестации оценивается уровень обученности «знать», «уметь», «владеть» в соответствии с запланированными результатами обучения и содержанием рабочей программы дисциплины:

– профессиональные знания студента могут проверяться при ответе на теоретические вопросы, выполнении тестовых заданий, практических работ,

– степень владения профессиональными умениями – при решении ситуационных задач, выполнении практических работ и других заданий.

4. Результаты выполнения заданий фиксируются в баллах. Общее количество баллов (макс. - 15 б.) складывается из:

– 5 баллов (33,3% от общей оценки) за выполнение практических заданий на выявление уровня обученности «уметь»,

– 5 баллов (33,3% от общей оценки) за выполнение практических заданий на выявление уровня обученности «владеть»,

– 3 балла (20% оценки) за ответы на теоретические вопросы,

– 2 балла (13,3% оценки) за ответы на дополнительные вопросы.

5. По итогам текущего контроля и промежуточной аттестации в соответствии с показателями и критериями оценивания компетенций определяется уровень сформированности компетенций студента и выставляется оценка по шкале оценивания.

1.4. Показатели и критерии оценивания компетенций, шкала оценивания

Компетенции	Показатели оценивания	Критерии оценивания компетенций				
		Высокий (верно и в полном объеме) 5 б.	Средний (с незначительными замечаниями) 4 б.	Низкий (на базовом уровне, с ошибками) 3 б.	Недостаточный (содержит большое количество ошибок/ответ не дан) – 2 б.	Итого:
Теоретические показатели						
ОПК-1 ПК-9	Знает основные методы принятия организационно-управленческих решений, основные методики взаимодействия с обществом, коллективом, партнерами в своей профессиональной деятельности; *Доклад*	Верно, и в полном объеме знает основные методы принятия организационно-управленческих решений, основные методики взаимодействия с обществом, коллективом, партнерами в своей профессиональной деятельности;	С незначительными замечаниями знает основные методы принятия организационно-управленческих решений, основные методики взаимодействия с обществом, коллективом, партнерами в своей профессиональной деятельности;	На базовом уровне, с ошибками знает основные методы принятия организационно-управленческих решений, основные методики взаимодействия с обществом, коллективом, партнерами в своей профессиональной деятельности;	Не знает основные методы принятия организационно-управленческих решений, основные методики взаимодействия с обществом, коллективом, партнерами в своей профессиональной деятельности;	*15*
	Знает современные методы управления информационной безопасности ИТ-инфраструктуры предприятия; *Доклад*	Верно, и в полном объеме знает современные методы управления информационной безопасности ИТ-инфраструктуры предприятия;	С незначительными замечаниями знает современные методы управления информационной безопасности ИТ-инфраструктуры предприятия;	На базовом уровне, с ошибками знает современные методы управления информационной безопасности ИТ-инфраструктуры предприятия;	Не знает современные методы управления информационной безопасности ИТ-инфраструктуры предприятия;	
	Знает специфику создания и развития ИТ-инфраструктуры предприятия *Доклад*	Верно, и в полном объеме знает специфику создания и развития ИТ-инфраструктуры	С незначительными замечаниями знает специфику создания и	На базовом уровне, с ошибками знает специфику создания и развития ИТ-инфраструктуры	Не знает специфику создания и развития ИТ-инфраструктуры предприятия	

		предприятия	развития ИТ-инфраструктуры предприятия	предприятия		
Практические показатели						
ОПК-1 *ПК-9*	Умеет анализировать и выбирать организационно-управленческие решения в своей деятельности, осознавать ответственность за принимаемые решения, добиваться поставленных задач во взаимодействии с обществом, коллективом, партнерами; *Лабораторная работа*	Верно, и в полном объеме может анализировать и выбирать организационно-управленческие решения в своей деятельности, осознавать ответственность за принимаемые решения, добиваться поставленных задач во взаимодействии с обществом, коллективом, партнерами;	С незначительными замечаниями может анализировать и выбирать организационно-управленческие решения в своей деятельности, осознавать ответственность за принимаемые решения, добиваться поставленных задач во взаимодействии с обществом, коллективом, партнерами;	На базовом уровне, с ошибками может анализировать и выбирать организационно-управленческие решения в своей деятельности, осознавать ответственность за принимаемые решения, добиваться поставленных задач во взаимодействии с обществом, коллективом, партнерами;	Не может анализировать и выбирать организационно-управленческие решения в своей деятельности, осознавать ответственность за принимаемые решения, добиваться поставленных задач во взаимодействии с обществом, коллективом, партнерами;	*10*
	Умеет обосновывать необходимость совершенствования управления информационной безопасностью предприятия, необходимость создания, развития и модернизации ИТ-инфраструктуры предприятия; *Лабораторная работа*	Верно, и в полном объеме может обосновывать необходимость совершенствования управления информационной безопасностью предприятия, необходимость создания, развития и модернизации ИТ-	С незначительными замечаниями может обосновывать необходимость совершенствования управления информационной безопасностью предприятия, необходимость	На базовом уровне, с ошибками может обосновывать необходимость совершенствования управления информационной безопасностью предприятия, необходимость создания, развития и модернизации ИТ-	Не может обосновывать необходимость совершенствования управления информационной безопасностью предприятия, необходимость создания, развития и модернизации ИТ-инфраструктуры	

		инфраструктуры предприятия;	создания, развития и модернизации ИТ-инфраструктуры предприятия;	инфраструктуры предприятия;	предприятия;	
Владеет						
ОПК-1 *ПК-9*	Владеет навыками выработки организационно-управленческих решений, ответственного их исполнения во взаимодействии с обществом, коллективом, партнерами; *Самостоятельная работа, контрольная работа*	Верно, и в полном объеме владеет навыками выработки организационно-управленческих решений, ответственного их исполнения во взаимодействии с обществом, коллективом, партнерами;	С незначительными замечаниями владеет навыками выработки организационно-управленческих решений, ответственного их исполнения во взаимодействии с обществом, коллективом, партнерами;	На базовом уровне, с ошибками владеет навыками выработки организационно-управленческих решений, ответственного их исполнения во взаимодействии с обществом, коллективом, партнерами;	Не владеет навыками выработки организационно-управленческих решений, ответственного их исполнения во взаимодействии с обществом, коллективом, партнерами;	*10*
	Владеет навыками консультирования клиентов и партнеров по вопросам совершенствования управления информационной безопасностью и бизнес процессов ИТ- инфраструктуры предприятия *Самостоятельная работа, контрольная работа*	Верно, и в полном объеме владеет навыками консультирования клиентов и партнеров по вопросам совершенствования управления информационной безопасностью и бизнес процессов ИТ-инфраструктуры предприятия	С незначительными замечаниями владеет навыками консультирования клиентов и партнеров по вопросам совершенствования управления информационной безопасностью и бизнес процессов ИТ-инфраструктуры предприятия	На базовом уровне, с ошибками владеет навыками консультирования клиентов и партнеров по вопросам совершенствования управления информационной безопасностью и бизнес процессов ИТ-инфраструктуры предприятия	Не владеет навыками консультирования клиентов и партнеров по вопросам совершенствования управления информационной безопасностью и бизнес процессов ИТ- инфраструктуры предприятия	
						35

Шкала оценивания:

Оценка	Баллы	Уровень сформированности компетенции
отлично	30-35	высокий
хорошо	25-29	хороший
удовлетворительно	18-24	достаточный
неудовлетворительно	17 и менее	недостаточный

2. Типовые контрольные задания для оценки результатов обучения по дисциплине и иные материалы для подготовки к промежуточной аттестации

2.1 Материалы для подготовки к промежуточной аттестации

Вопросы к экзамену:

1. Основные задачи, которые выполняют ИАС.
2. Роль и место анализа в принятии решений.
3. Проблемы анализа в свете использования информационных технологий.
4. Содержание аспекта сбора и хранения данных.
5. Содержание аспекта анализа данных и предоставления результатов анализа пользователям.
6. Классификация средств выполнения анализа с помощью ИТ.
7. Состав информационных технологий и информационных систем на предприятии и из внешней среды – источников данных для сосредоточения в информационном хранилище или непосредственно для анализа.
8. Понятие и структура информационного пространства.
9. Элементы структуры информационного пространства.
10. Понятия показателя и реквизитов.
11. Пространственная интерпретация понятия показатель.
12. Содержание экономических показателей.
13. Виды систем экономических показателей.
14. Рекомендации по структуризации информационного пространства предприятия при создании ИАС.
15. Принципы гибкой архитектуры данных и открытых систем, которыми руководствуются при создании ИАС.
16. Информационный обмен, связанный с аналитической работой.
17. Понятие информационного хранилища.
18. Принципы построения информационных хранилищ.
19. Требования к качеству данных и способы его обеспечения при загрузке в информационное хранилище.
20. Проблемы, разрешаемые при приведении данных к единой структуре информационного хранилища.
21. Концепции построения структур хранилищ данных.
22. Назначение, состав и выполняемые функции базы метаданных – репозитория ИХ.
23. Принципы создания репозитория ИХ.
24. Элементы моделей данных ИХ (факт-таблица, таблицы измерений, консольные таблицы).
25. Назначение, состав и выполняемые функции базы метаданных – репозитория ИХ.
26. Принципы создания репозитория ИХ.

27. Элементы моделей данных ИХ (факт-таблица, таблицы измерений, консольные таблицы).

28. Схемы представления – модели многомерных данных.

29. Признаки OLAP-систем.

30. Типы многомерных OLAP-систем.

31. Классификация ИТ-анализа по режиму и темпу.

32. Задачи и содержание оперативного (OLAP) анализа.

33. Содержание понятия «знания», классификация видов знаний.

34. Интеллектуальный анализ данных (Data mining), цели и решаемые задачи.

35. Состав и содержание специфических задач интеллектуального анализа.

36. Особенности средств интеллектуального анализа данных.

37. Содержание методики нечёткая логика.

38. Сущность кластеризации данных, её отличие от классификации.

39. Области применения методов интеллектуального анализа.

40. Системы рассуждений на основе анлогичных случаев.

41. Классификационные и регрессионные деревья решений.

42. Байесовское обучение (ассоциации).

43. Генетические алгоритмы.

44. Эволюционное программирование

45. Понятие искусственного интеллекта и интеллектуальных информационных систем.

46. Системы с интеллектуальным интерфейсом.

47. Экспертные системы, их виды и особенности.

48. Самообучающиеся системы и извлечение знаний из данных.

49. Адаптивные информационные системы, принципы адаптации на основе модели предметной области.

50. Теоретические основы систем управления знаниями.

51. Принципы управления знаниями.

52. Основные подсистемы управления знаниями.

53. Источники знаний – эксперты и системы хранения данных.

54. Способы извлечения знаний из источников.

55. Роль онтологии знаний в концептуальном моделировании проблемной области.

56. Состав программных инструментальных средств ИАС.

57. Средства сбора и доработки данных.

58. Средства оперативного OLAP– анализа.

59. Средства интеллектуального анализа данных.

60. Управление информационно-аналитическими системами.

61. Задачи и средства администрирования ИАС.

62. Технологии загрузки данных в информационное хранилище.

Типовые контрольные задания:

Задание 1. Определите в каких формах представлена информация на вашей домашней ЭВМ. Опишите, как обеспечивается информационная безопасность вашей ПЭВМ и отвечает ли современным требованиям развития систем безопасности.

Задание 2. Определите и классифицируйте угрозы безопасности вашего домашнего ПЭВМ.

Задание 3. В приведенном вами примере организации защиты информации найдите недостатки системы, предложите пути их устранения.

Задание 4. Предложите схему удаленного администрирования сети филиала. Выбор схемы и соответствующего ПО обоснуйте.

Задание 5. Опишите каким образом осуществлено разграничение доступа к информационным ресурсам на вашей ПЭВМ, в случае отсутствия его обоснуйте.

Задание 6. Раскройте сущность приведенного вируса.

№ варианта	Вид вируса
1, 5, 9 ,13	Стелс-вирус
2, 6, 10,14	Boot - вирус
3, 7, 11,15	Макровирус
4, 8, 12,16	Вирус-червь

Задание 7. Опишите антивирусные программы, которые вы использовали и используете в данный момент. Ваш выбор обоснуйте.

Задание 8. Приведите примеры, когда вам приходилось восстанавливать удаленную информацию. Опишите и обоснуйте логическую разбивку вашего жесткого диска.

Задание 9. Определите какие организационные меры вы используете в своем быту, приведите примеры использования в учебном процессе.

Задание 10. Определите какими нормативными документами ограничен круг задач, решаемых вами с использованием вашей домашней ПЭВМ.

Образцы тестовых заданий для проведения текущего контроля и промежуточной аттестации по итогам освоения дисциплины, а также для контроля самостоятельной работы:

1. Информационная безопасность - это комплекс мероприятий, обеспечивающий для охватываемой им информации следующие факторы:

а) конфиденциальность
б) целостность
в) доступность
г) учет
д) неотрекаемость
е) мобильность

2. ... - это набор формальных правил, которые регламентируют функционирование механизма информационной безопасности.

а) Политика
б) Идентификация
в) Аутентификация
г) Контроль доступа
д) Авторизация

3. ... - распознавание каждого участника процесса информационного взаимодействия перед тем, как к нему будут применены какие бы то ни было понятия информационной безопасности.

а) Политика
б) Идентификация
в) Аутентификация
г) Контроль доступа
д) Авторизация

4. ... - обеспечение уверенности в том, что участник процесса обмена информацией определен верно, т.е. действительно является тем, чей идентификатор он предъявил.

а) Политика
б) Идентификация
в) Аутентификация
г) Контроль доступа
д) Авторизация

5. ... - создание и поддержание набора правил, определяющих каждому участнику процесса информационного обмена разрешение на доступ к ресурсам и уровень этого доступа.

а) Политика
б) Идентификация
в) Аутентификация

г) Контроль доступа
д) Авторизация

6. ... - формирование профиля прав для конкретного участника процесса информационного обмена из набора правил контроля доступа.
а) Политика
б) Идентификация
в) Аутентификация
г) Контроль доступа
д) Авторизация

7. ... - обеспечение соответствия возможных потерь от нарушения информационной безопасности затратам на их построение.
а) Реагирование на инциденты
б) Управление конфигурацией
в) Управление пользователями
г) Управление рисками
д) Обеспечение устойчивости

8. ... - поддержание среды информационого обмена в минимально допустимом работоспособном состоянии и сооответствии требованиям информационной безопасности в услових деструктивны внешних или внутренних воздействий.
а) Реагирование на инциденты
б) Управление конфигурацией
в) Управление пользователями
г) Управление рисками
д) Обеспечение устойчивости

Литература для подготовки к экзамену:

а) основная литература

1. Информационная безопасность и защита информации: Учебное пособие / Баранова Е. К., Бабаш А. В. - 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с. - Режим доступа: http://znanium.com/catalog/product/495249

2. Информационная безопасность предприятия: Учебное пособие / Гришина Н.В., - 2-е изд., доп - М.: Форум, НИЦ ИНФРА-М, 2016. - 240 с.- Режим доступа: http://znanium.com/catalog/product/544554

б) дополнительная литература

1. Башлы, П. Н. Информационная безопасность и защита информации : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - Режим доступа: http://znanium.com/catalog/product/405000

Промежуточная аттестация

2.2. Комплект экзаменационных билетов для проведения промежуточной аттестации

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОБРАЗОВАТЕЛЬНАЯ
ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
ЦЕНТРОСОЮЗА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ УНИВЕРСИТЕТ КООПЕРАЦИИ»
КАЗАНСКИЙ КООПЕРАТИВНЫЙ ИНСТИТУТ (ФИЛИАЛ)

Направление подготовки: 38.03.05 Бизнес-информатика
Направленность: «Электронный бизнес»
Дисциплина: «Информационная безопасность»

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Основные задачи, которые выполняют ИАС.
2. Антивирусные средства.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 2

1. Классификация средств выполнения анализа с помощью ИТ..
2. Межсетевые экраны

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 3

1. Понятие и структура информационного пространства
2. Организационно-технические и режимные меры и методы защиты информации. 149-ФЗ от 27.06.2006г.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 4

1. Понятие об информационных системах.
2. Организационно-технические и режимные меры и методы защиты информации. 152-ФЗ от 27.06.2006г.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 5

1. Анализаторы протоколов.
2 Объекты защиты информации. Защита информации ограниченного доступа: государственная тайна, коммерческая тайна.

Промежуточная аттестация

Комплект тестовых заданий для проведения экзамена по дисциплине

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОБРАЗОВАТЕЛЬНАЯ
ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
ЦЕНТРОСОЮЗА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ УНИВЕРСИТЕТ КООПЕРАЦИИ»
КАЗАНСКИЙ КООПЕРАТИВНЫЙ ИНСТИТУТ (ФИЛИАЛ)

Направление подготовки: 38.03.05 Бизнес-информатика
Направленность: «Электронный бизнес»
Дисциплина: «Информационная безопасность»

Тестовые задания для проверки уровня обученности **ЗНАТЬ:**

1. При обнаружении файлового вируса…

а) Следует удалить все файлы, хранящиеся на жестком диске компьютера

б) Компьютер от сети отключать не следует, достаточно на период лечения убедиться в том, что соответствующий редактор неактивен

в) Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются

г) Компьютер необходимо отключить от сети и проинформировать системного администратора

2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

а) Сотрудники
б) Хакеры
в) Контр агенты
г) Атакующие

3. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

а) Руководство
б) Администраторы
в) Пользователи
г) Владельцы данных

4. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

а) Поддержка высшего руководства
б) эффективные защитные меры и методы их внедрения
в) актуальные и адекватные политики и процедуры безопасности

г) проведение тренингов по безопасности для всех сотрудников

5. Информационная технология это

а) Совокупность технических средств.

б) Совокупность программных средств.

в) Совокупность организационных средств.

г) Множество информационных ресурсов

д) Совокупность операций по сбору, обработке, передачи и хранению данных с использованием методов и средств автоматизации.

Тестовые задания для проверки уровня обученности **УМЕТЬ, ВЛАДЕТЬ:**

1. Для управления взаимоотношениями с клиентами фирмы используют…

а) глобальные распределительные системы GDS (Global Distribution System)

б) системы поддержки принятия решений (СППР)

в) систему передачи информации и совершения платежей SWIFT (Society for Worldwide Interbank Financial Telecommunications)

г) CRM-системы (Customer Relationship Management)

2. Что такое политики безопасности?

а) Пошаговые инструкции по выполнению задач безопасности

б) Общие руководящие требования по достижению определенного уровня безопасности

в) Широкие, высокоуровневые заявления руководства

г) Детализированные документы по обработке инцидентов безопасности

3. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

а) Анализ затрат\выгод

б) Анализ рисков

в) Результаты ALE

г) Выявление уязвимостей и угроз, являющихся причиной риска

4. Среди нижеперечисленных выделите главную причину существования

а) многочисленных угроз информационной безопасности.

б) просчеты при администрировании информационных систем;

в) необходимость постоянной модификации информационных систем;

г) сложность современных информационных систем.

5. Дублирование сообщений является угрозой:
а) доступности;
б) конфиденциальности;
в) целостности.

2.3. Критерии оценки для проведения экзамена по дисциплине

После завершения тестирования на экзамене на мониторе компьютера высвечивается результат – процент правильных ответов. Результат переводится в баллы и суммируется с текущими семестровыми баллами.

Максимальная сумма (100 баллов), набираемая студентом по дисциплине, предусматривающей в качестве формы промежуточной аттестации экзамен, включают две составляющие.

Первая составляющая – оценка регулярности и своевременности качества выполнения студентом учебной работы по изучению дисциплины в течение семестра (сумма не более 60 баллов).

Вторая составляющая – оценка знаний студента на экзамене (не более 40 баллов).

Перевод полученных итоговых баллов в оценки осуществляется по следующей шкале:

- с 86 до 100 баллов – «отлично»;
- с 71 до 85 баллов – «хорошо»;
- с 50 до 70 баллов – «удовлетворительно»

Если студент при тестировании отвечает правильно менее, чем на 50 %, то автоматически выставляется оценка «неудовлетворительно» (без суммирования текущих рейтинговых баллов), а студенту назначается переэкзаменовка в дополнительную сессию.

2.4. Методические материалы, определяющие процедуру оценивания по дисциплине

Общая процедура оценивания определена Положением о фондах оценочных средств.

1. Процедура оценивания результатов освоения программы дисциплины включает в себя оценку уровня сформированности общекультурных и профессиональных компетенций студента, уровней обученности: «знать», «уметь», «владеть».

2. При сдаче экзамена:

– профессиональные знания студента могут проверяться при ответе на теоретические вопросы, при выполнении тестовых заданий, практических работ;

– степень владения профессиональными умениями, уровень сформированности компетенций (элементов компетенций) – при решении ситуационных задач, выполнении практических работ и других заданий.

3. Результаты промежуточной аттестации фиксируются в баллах. Общее количество баллов складывается из следующего:

- до 60% от общей оценки за выполнение практических заданий,
- до 30% оценки за ответы на теоретические вопросы,
- до 10% оценки за ответы на дополнительные вопросы.

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОБРАЗОВАТЕЛЬНАЯ
ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
ЦЕНТРОСОЮЗА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ УНИВЕРСИТЕТ КООПЕРАЦИИ»
КАЗАНСКИЙ КООПЕРАТИВНЫЙ ИНСТИТУТ (ФИЛИАЛ)

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ТЕКУЩЕЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки: 38.03.05 Бизнес-информатика
Направленность: «Электронный бизнес»

1. Материалы для текущего контроля

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОБРАЗОВАТЕЛЬНАЯ
ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
ЦЕНТРОСОЮЗА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ УНИВЕРСИТЕТ КООПЕРАЦИИ»
КАЗАНСКИЙ КООПЕРАТИВНЫЙ ИНСТИТУТ (ФИЛИАЛ)

КОМПЛЕКТ ЗАДАНИЙ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

по дисциплине «Информационная безопасность»

Контрольные работы по дисциплине «Информационная безопасность» состоят из тестовых вопросов

1. Под информационной безопасностью РФ понимается:

а) состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства

б) состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов гражданина, семьи и государства

в) состояние защищенности ее международных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства

2. Интересы личности в информационной сфере это:

а) реализация конституционных прав человека и гражданина на доступ к информации

б) использование информации в духовном обновлении личности

в) защита информации при взаимовыгодном международном сотрудничестве

3. Интересы общества в информационной сфере это:

а) упрочение демократии, создании правового социального государства

б) реализация информации в интересах физического, духовного и интеллектуального развития человека

в) развитие Российской информационной инфраструктуры

4. Интересы государства в информационной сфере

а) развитие равноправного и взаимовыгодного международного сотрудничества

б) достижение и поддержание общественного согласия

в) обеспечение конституционных прав духовной личности

5. Виды угроз информационной безопасности Российской Федерации

а) угрозы конституционным правам; информационному обеспечению государственной политики Российской Федерации; развитию отечественной индустрии информации; безопасности информационных систем

б) угрозы духовным правам; геополитическому обеспечению государственной политики Российской Федерации; развитию отечественной индустрии информации; безопасности средств массовой информации

в) угрозы внутренним и внешним потребностям человека; информационно-коммуникационному обеспечению государственной политики Российской Федерации; развитию международной индустрии информации; безопасности средств массовой информации

6. Источники угроз информационной безопасности Российской Федерации бывают:

а) наружние и внутренние

б) основные и базовые

в) внутренние и внешние

7. Общие методы обеспечения информационной безопасности Российской Федерации состоят из следующих факторов:

а) юридических, организационно-методических, человеческих

б) правовых, организационно-технических, экономических

в) законных, организационно-информационных, хозяйственных

8. Что относится к базовым принципам информационной безопасности:

а) целостность, конфиденциальность, доступность

б) нормативно-правовой, программный, исполнительный

в) организационный, административный, программный

9. К формам защиты информации не относится…

а) правовая

б) организационно-техническая

в) страховая

г) аналитическая

10. Организация методов обеспечения информационной безопасности Российской Федерации начинается с выяснения

а) объектов отношений

б) предметов отношений

в) субъектов отношений

11. Угроза информационной безопасности – это

а) потенциальная возможность определенным образом нарушить информационную безопасность

б) специально написанная программа, которая может приписывать себя к другим программам

в) несанкционированное использование информации

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

а) «для служебного пользования»

б) «секретно»

в) «совершенно секретно»

г) «особой важности»

13. Что из перечисленного не относится к числу основных аспектов информационной безопасности:

а) доступность

б) целостность

в) защита от копирования

г) конфиденциальность

14. Информационная безопасность – это дисциплина:

а) комплексная

б) техническая

в) программистская

15. На законодательном уровне информационной безопасности особенно важны:

а) направляющие и координирующие меры

б) ограничительные меры

в) меры по обеспечению информационной независимости

16. Политика безопасности:

а) фиксирует правила разграничения доступа

б) отражает подход организации к защите своих информационных активов

в) описывает способы защиты руководства организации

17. Основным документом, на основе которого проводится политика информационной безопасности предприятия, является:

а) закон РФ «Об информации, информатизации и защите информации»

б) перечень критерии в оценки надежных компьютерных систем («Оранжевая книга»)

в) программа информационной безопасности предприятия

18. Закон «Об информации, информатизации и защите информации» в Российской Федерации был принят в #### году.

а) 1995
б) 1998
в) 2000

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

а) средства нанесения контратаки с помощью информационного оружия

б) механизмы защиты пользователей от различных типов и уровней угроз для национальной информационной инфраструктуры

в) признаки, сигнализирующие о возможном нападении

г) процедуры оценки уровня и особенностей атаки против национальной инфраструктуры в целом и отдельных пользователей

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

а) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации реализацию права на доступ к информации»

б) соблюдение норм международного права в сфере информационной безопасности

в) выявление нарушителей и привлечение их к ответственности

г) соблюдение конфиденциальности информации ограниченного доступа

д) разработку методов и усовершенствование средств информационной безопасности

21. Какие методы обеспечения информационной безопасности Российской Федерации направлены на создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи?

а) правовые

б) организационно-технические

в) экономические

22. На решение каких вопросов направлена система лицензирования деятельности в области защиты государственной тайны?

а) на выполнение требований к организациям и лицам, занимающимся вопросами защиты государственной тайны

б) на повышение экономической эффективности деятельности в области защиты государственной тайны

в) на обеспечение правовых основ деятельности в области защиты государственной тайны

г) на решение проблемы надлежащего финансирования работ в области защиты государственной тайны

23. Частью какой, более общей системы, является система обеспечения информационной безопасности Российской Федерации?

а) системы защиты национальных интересов страны

б) системы обороны страны

в) системы защиты прав граждан страны

г) системы обеспечения национальной безопасности страны

24.Европейскиекритериибезопасностикомпьютерныхсистемрассматриваютследующиесоставляющиеинформационнойбезопасности:

а) конфиденциальность

б) целостность

в) гарантированность

г) доступность

д) надежность

Критерии оценки:

Студент аттестован, если правильно ответил более чем на 10 вопросов.

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОБРАЗОВАТЕЛЬНАЯ
ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
ЦЕНТРОСОЮЗА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ УНИВЕРСИТЕТ КООПЕРАЦИИ»
КАЗАНСКИЙ КООПЕРАТИВНЫЙ ИНСТИТУТ (ФИЛИАЛ)

ТЕМЫ ДОКЛАДОВ

по дисциплине «Информационная безопасность»

1. "Практика использования электронной цифровой подписи. Основные принципы обеспечения информационной безопасности с использованием инфраструктуры открытых ключей. Архитектура удостоверяющего центра на базе Крипто-Про CSP. Использование ЭЦП для организации защищенного электронного документооборота
2. "Управление безопасностью в корпоративных распределенных вычислительных системах и сетях связи. Практические аспекты"
3. "Защита документов и товаров с использованием электронной цифровой подписи"
4. "Комплексные решения по защите информации с использованием РИК"
5. "Технологии AMD 2003-2005 годов с точки зрения безопасности планирования инфраструктуры организации и эффективности капиталовложений"
6. "Основные современные аспекты нарушений работоспособности информационных систем"
7. "Перспективы развития аппаратных средств защиты от несанкционированного доступа к информации"
8. "Аспекты информационной безопасности"
9. "Практика использования электронной цифровой подписи. Основные принципы обеспечения информационной безопасности с использованием инфраструктуры открытых ключей. Архитектура удостоверяющего центра на базе Крипто-Про CSP. Использование ЭЦП для организации защищенного электронного документооборота."

Критерии оценки:

- оценка «отлично» выставляется студенту, если задание выполнено верно и в полном объеме;
- оценка «хорошо» выставляется студенту, если задание выполнено с незначительными замечаниями;
- оценка «удовлетворительно» выставляется, если задание выполнено на базовом уровне, но с ошибками;
- оценка «неудовлетворительно» выставляется, если содержится большое количество ошибок, задание не выполнено.

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОБРАЗОВАТЕЛЬНАЯ
ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
ЦЕНТРОСОЮЗА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ УНИВЕРСИТЕТ КООПЕРАЦИИ»
КАЗАНСКИЙ КООПЕРАТИВНЫЙ ИНСТИТУТ (ФИЛИАЛ)

ЛАБОРАТОРНЫЕ РАБОТЫ

Лабораторная работа №1

Тема: Поиск законодательства РФ в области защиты информации с использованием Интернет-ресурсов.

Цель: Научиться использовать Интернет-ресурсы для поиска необходимой информации.

Задание

1. Используя поисковые системы, компьютерную справочно-правовую система "Консультант плюс", найти основные законодательные документы РФ в сфере информационной безопасности:

a) "Доктрина информационной безопасности Российской Федерации" (утв. Президентом РФ 09.09.2000 N Пр-1895);

b) Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 31.12.2014) "Об информации, информационных технологиях и о защите информации" (с изм. и доп.). Статья 2. Основные понятия, используемые в настоящем Федеральном законе;

c) "Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года" (утв. Президентом РФ 24.07.2013 N Пр-1753)

Используя найденные документы, заполнить следующую таблицу:

Искомый элемент	**Описание (определение)**
Информационная безопасность Российской Федерации	
Интересы личности в информационной сфере	
Интересы общества в информационной сфере	
Интересы государства в информационной сфере	
Основные составляющие национальных интересов Российской Федерации в информационной сфере (четыре составляющих)	
Виды угроз информационной безопасности Российской Федерации	
Внешние источники угроз информационной безопасности Российской Федерации	
Внутренние источники угроз информационной безопасности Российской Федерации	
Информационно-телекоммуникационная сеть	
Доступ к информации	
Предоставление информации	

Искомый элемент	Описание (определение)
Распространение информации	
Электронное сообщение	
Документированная информация	
Электронный документ	
Сайт в сети "Интернет"	
Владелец сайта в сети "Интернет"	
Международная информационная безопасность	
Система международной информационной безопасности	

2. Используя поисковые системы, компьютерную справочно-правовую система "Консультант плюс", найти "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 30.12.2015). Глава 28. Преступления в сфере компьютерной информации. Записать статьи УК из Главы 28.

Лабораторная работа №2

Тема: Составление досье с использованием интернет-ресурсов для оценки воздействия ИКТ-технологий на неприкосновенность частной жизни.

Цель: Воспитание ответственного отношения к информационной деятельности, связанной с обработкой и хранением информации.

Приобретение опыта профилактической и предупреждающей деятельности по отношению к информационным угрозам на уровне личной информационной безопасности

Задание

Собрать и систематизировать как можно больше информации о друге с использованием общедоступных Интернет-ресурсов, оценить угрозу злоумышленного применения информации и выработать рекомендации по обеспечению необходимого уровня безопасности частной жизни в мире цифровых зависимостей.

Методические указания

Для выполнения лабораторной работы студенты разбиваются на пары.

1. Найти как можно больше личной информации о коллеге, используя общедоступные сетевые ресурсы:

1) поисковые системы bing.ru, google.ru, yandex.ru, rambler.ru, aport.ru и др.;

2) социальные сети: vkontakte.ru, odnoklassniki.ru, moikrug.ru, professionali.ru, linkedin.com,facebook.com и др.;

3) сервисы онлайн-блогов: livejournal.com, blogs.mail.ru, blogs.yandex.ru, blog.ru, www.blogdir.ru;

4) сайты профессиональных сообществ;

5) сайты вузов.

2. Создать с использованием собранной информации досье со следующими основными разделами:

1) ФИО, дата рождения, семейное положение, место проживания, контакты;
2) профессия, области профессиональных интересов, жизненные цели;
3) круг общения: родственники, друзья, коллеги, знакомые;
4) посещаемые места, пристрастия в еде, одежде, музыке и др.;
5) наличие машины;
6) распорядок дня;
7) фотографии;
8) другое.

Досье оформить в виде презентации.

3. Оценить возможность использования найденной информации злоумышленниками, например:

1) телефонными террористами;
2) мошенниками;
3) похитителями номеров банковских карт;
4) распространителями рекламной продукции и т.д.

Оформить в виде текстового документа.

4. Передать собранные материалы "коллеге" и получить досье с информацией о себе.

5. Оценить уровень конфиденциальности, актуальности и достоверности собранной информации.

6. Проанализировать выводы коллеги о возможности использования найденной информации злоумышленниками.

7. Оценить уровень влияния цифровых технологий на свою частную жизнь и продумать шаги по обеспечению желаемого уровня безопасности.

Лабораторная работа №3

Тема: Решение ситуационных задач

Задача 1:

Сотрудник научно-исследовательского института приборостроения скопировал схемы, чертежи и графики прибора с целью продажи этой информации зарубежной фирме-производителю.

Правомерно ли это?

Указания к выполнению: Используя компьютерную справочно-правовую систему "Консультант плюс", найти "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 13.07.2015, с изм. от 16.07.2015) (с изм. и доп., вступ. в силу с 25.07.2015). Ознакомиться с Главой 28. Преступления в сфере компьютерной информации.

Используя найденные статьи "Уголовного кодекса Российской Федерации", решить ситуационную задачу.

Задача 2:

Будет ли удовлетворен иск компании «Интермедиа» о привлечении к уголовной ответственности гражданина Р.И.Сизова и выплате им фирме денежной компенсации, если он внедрил в компьютерную сеть компании программу, действие которой заключается в уничтожении исполняемых файлов в какой-либо компьютерной сети?

Функционирование данной программы принесло убытки различным организациям на общую сумму 670 000 рублей.

Указания к выполнению: Используя компьютерную справочно-правовую систему "Консультант плюс", найти "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 13.07.2015, с изм. от 16.07.2015) (с изм. и доп., вступ. в силу с 25.07.2015). Ознакомиться с Главой 28. Преступления в сфере компьютерной информации.

Используя найденные статьи "Уголовного кодекса Российской Федерации", решить ситуационную задачу.

Задача 3:

Гражданин Серегин разработал в соавторстве с гражданином Зинуровым информационно-справочную систему "Энциклопедия. Реки Сибири". Финансовую поддержку программных разработок вышеупомянутым гражданам оказал гражданин Кулагин. Граждане Серегин и Зинуров 15 апреля 2015 года оформили свое авторство на данную информационную систему. В феврале 2015 года данный программный продукт был выпущен под авторством гражданина Кулагина.

Имеет ли место в данной ситуации нарушение авторского права граждан Серегина и Зинурова?

Указания к выполнению: Используя компьютерную справочно-правовую систему "Консультант плюс", найти закон "О правовой охране программ для ЭВМ и баз данных".

Используя найденный закон, решить ситуационную задачу.

Задача 4:

Определите, будет ли электронная подпись равнозначной собственноручной подписи, если подтверждена подлинность электронной цифровой подписи в электронном документе.

Указания к выполнению: Используя компьютерную справочно-правовую систему "Консультант плюс", найти закон "Об электронной цифровой подписи".

Используя найденный закон, решить ситуационную задачу.

Лабораторная работа №4-5

Тема: Основы криптографии. Шифры замены (подстановки): шифр

Цезаря.

Цель: научиться разрабатывать криптографическую защиту информации, содержащейся в строке, с помощью шифра Цезаря.

Задание: разработать криптографическую защиту информации, содержащейся в строке (строка вводится с клавиатуры), с помощью шифра Цезаря.

Для этого:

1. Определить алфавит криптосистемы (открытого текста и шифртекста). Например, русский, английский, ASCII.
2. Разработать алгоритмы шифрования и дешифрования открытого текста. Определить ключ.
3. Написать программу, реализующую шифрование открытого текста, состоящего из символов заданного алфавита. Провести тестирование программы.
4. Написать программу для реализации алгоритма дешифрования полученного шифртекста. Провести тестирование программы.

Методические указания

1. В качестве алфавита криптосистемы будет использоваться русский алфавит (строчные буквы).
2. Определить коды символов русского алфавита. Для этого необходимо написать программу, которая выводит коды ASCII символов русского алфавита (используется функция ord) и проследить закономерность.
3. Алгоритм шифрования (шифр Цезаря): каждая буква заменяется на следующую через одну после нее. Алфавит замыкается, поэму букву "ю" необходимо заменить на "а", а букву "я" на "б". В качестве ключа выступает число, на которое надо сдвигать буквы, а данном случае это число 2.
4. При написании программы шифрования необходимо предусмотреть: ввод строки с клавиатуры; преобразование всех букв в строчные буквы (функция LowerCase); удаление из строки пробелов.
5. В программе шифрования необходимо просматривать все символы преобразованной строки (после удаления пробелов) посимвольно (используется цикл с параметром). Каждый символ необходимо преобразовывать в код ASCII (используется функция ord), затем выполнять действия по преобразованию кода согласно алгоритму шифрования. После этого необходимо код преобразовать в символ (используется функция chr), который будет использоваться для формирования новой строки – шифр кода. Для проверки программы шифрования введите с клавиатуры строку 'Я иду в институт'. После шифрования должен быть получен следующий результат: 'бкжхдкпуфкфхф'.
6. В программе дешифрования необходимо выполнить обратные преобразования. Для проверки программы дешифрования введите с

клавиатуры строку 'дуздэсрнпзпрдзтпррфнкщпр'. Прочитайте полученный результат.

Лабораторная работа № 6-7

Тема: симметричные криптосистемы.

Цель работы: научиться разрабатывать криптографическую защиту информации, содержащейся в строке, с помощью шифрующей таблицы с перестановкой по ключу – размеру таблицы.

Задание: разработать криптографическую защиту информации, содержащейся в строке "**прилетаю восьмого**", с помощью шифрующей таблицы с перестановкой по ключу – размеру таблицы.

Для этого:

1. Определить алфавит криптосистемы (открытого текста и шифртекста) так, чтобы он включал в себя символы используемого в примере открытого текста. Например, русский, английский, ASCII.
2. Задать ключ в виде размера таблицы.
3. Разработать алгоритмы шифрования и дешифрования открытого текста.
4. Написать программу, реализующую шифрование на заданном ключе открытого текста, состоящего из символов заданного алфавита. Открытый текст и шифртекст должны быть представлены отдельными строками. Провести тестирование программы.
5. Написать программу для реализации алгоритма дешифрования полученного файла шифртекста при известном ключе. Провести тестирование программы.

Критерии оценки:

- оценка «отлично» выставляется студенту, если задание выполнено верно и в полном объеме;
- оценка «хорошо» выставляется студенту, если задание выполнено с незначительными замечаниями;
- оценка «удовлетворительно» выставляется, если задание выполнено на базовом уровне, но с ошибками;
- оценка «неудовлетворительно» выставляется, если содержится большое количество ошибок, задание не выполнено.

2. Материалы для проведения текущей аттестации

Текущая аттестация 1

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОБРАЗОВАТЕЛЬНАЯ
ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
ЦЕНТРОСОЮЗА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ УНИВЕРСИТЕТ КООПЕРАЦИИ»
КАЗАНСКИЙ КООПЕРАТИВНЫЙ ИНСТИТУТ (ФИЛИАЛ)

КОМПЛЕКТ ЗАДАНИЙ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ АТТЕСТАЦИИ №1
(в форме контрольной работы)

по дисциплине «Информационная безопасность»

1. Под угрозой безопасности информации понимается:

а) атака на информацию со стороны злоумышленника

б) потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, утрате целостности, конфиденциальности или доступности информации

в) не санкционированный доступ к информации, который может привести к нарушению целостности системы компьютерной безопасности

2. Все множество потенциальных угроз безопасности информации в КС может быть разделено на следующие классы:

а) случайные угрозы

б) потенциальные угрозы

в) преднамеренные угрозы

г) предсказуемые угрозы

Угрозы какого класса приводят к наибольшим потерям информации?

а) случайные

б) преднамеренные

3. Что понимается под возможным каналом утечки информации?

а) способ, позволяющий нарушителю получить доступ к хранящейся или обрабатываемой информации

б) техническое средство, с помощью которого нарушитель может получить доступ к хранящейся или обрабатываемой информации

в) комплекс программных и/или аппаратных средств, позволяющих осуществлять передачу данных от источника информации к нарушителю

4. С помощью каких типов средств может происходить утечка информации по возможному каналу ?

а) данные

б) человек
в) компьютерная сеть
г) программа
д) аппаратура

5. При хранении, поддержании и предоставлении доступа к любому информационному ресурсу его владелец, либо уполномоченное им лицо, накладывает явно либо само очевидно набор правил по работе с ней. Умышленное их нарушение классифицируется как на информацию.
а) атака
б) нападение
в) вмешательство
г) покушение

6. Укажите основные виды случайных угроз:
а) Стихийные бедствия и аварии
б) Сбои и отказы технических средств
в) Ошибки при разработке компьютерных систем
г) Алгоритмические и программные ошибки
д) Ошибки пользователей и обслуживающего персонала
е) Электромагнитные излучения и наводки
ж) Вредительские программы

7. Перечислите основные виды преднамеренных угроз:
а) Алгоритмические и программные ошибки
б) Шпионаж и диверсии
в) Не санкционированный доступ (НСД) к информации
г) Электромагнитные излучения и наводки
д) Несанкционированная модификация структур
е) Стихийные бедствия и аварии
ж) Вредительские программы

8. Алгоритмические и программные ошибки относятся к _____ угрозам.
а) случайным
б) преднамеренным
в) потенциальным

9. Несанкционированный доступ к информации относится к _____ угрозам.
а) случайным
б) преднамеренным
в) потенциальным

10. Действие или последовательность действий, приводящее к реализации угрозы, называется:

а) атакой

б) нападением

в) покушением

11. Несанкционированным доступом, атакой называют:

а) случайные угрозы

б) специальные угрозы

в) преднамеренные угрозы

г) внешние угрозы

12. Выполнение операции (например, чтения или записи) теми, кто этого недолжен делать:

а) фактически угроза

б) угроза

в) атака

г) нарушение конфиденциальности

13. Некоторая неудачная характеристика системы (программная ошибка, несовершенство аппаратной технологии, неверная настройка), благодаря которой становится возможным нарушение того или иного аспекта безопасности это:

а) уязвимость

б) угроза

в) фактически угроза

г) атака

14. Процесс соблюдения (сохранения) трех аспектов безопасности это:

а) конфиденциальность информации

б) информационная безопасность

в) применение превентивных мер

г) защита всех этапов обработки информации

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

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

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

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

г) способна противостоять только внешним информационным угрозам

16. Конфиденциальность компьютерной информации – это…

а) предотвращение проникновения компьютерных вирусов в память ПЭВМ

б) свойство информации быть известной только допущенным и прошедшим проверку (авторизацию) субъектам системы

в) безопасность программного обеспечения

17. Угроза доступности данных возникают в том случае, когда…

а) объект не получает доступа к законно выделенному ему ресурсу

б) легальный пользователь передает или принимает платежные документы

в) случаются стихийные бедствия

18. Нарушение, искажение или уничтожение информации относится к…

а) активным угрозам

б) пассивным угрозам

в) активно- пассивным угрозам

19. Подслушивание, копирование, просмотр информации относится к _____ угрозам.

а) активным

б) пассивным

в) активно-пассивным

20. Перехват информации в технических каналах, внедрение электронных устройств перехвата, воздействие на парольно - ключевые системы, радиоэлектронное подавление линий связи и систем управления относятся к _____ угрозам.

а) информационным

б) программно-математическим

в) радиоэлектронным

г) физическим

21. Результатом реализации угроз информационной безопасности может быть…

а) изменение конфигурации периферийных устройств

б) несанкционированный доступ к информации

в) уничтожение устройств ввода-вывода информации

22. Основные угрозы доступности информации:

а) непреднамеренные ошибки пользователей

б) злонамеренное изменение данных

в) хакерская атака

г) отказ программного и аппаратного обеспечения

д) разрушение или повреждение помещений

е) перехват данных

23. Вид угрозы действия, направленного на несанкционированное использование информационных ресурсов, не оказывающего при этом влияния на её функционирование – _____угроза

а) активная

б) пассивная

24. Преднамеренная угроза безопасности информации

а) кража

б) наводнение

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

г) ошибка разработчика

Критерии оценки:

Студент аттестован, если правильно ответил более чем на 15 вопросов.

Текущая аттестация 2

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОБРАЗОВАТЕЛЬНАЯ
ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
ЦЕНТРОСОЮЗА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ УНИВЕРСИТЕТ КООПЕРАЦИИ»
КАЗАНСКИЙ КООПЕРАТИВНЫЙ ИНСТИТУТ (ФИЛИАЛ)

КОМПЛЕКТ ЗАДАНИЙ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ АТТЕСТАЦИИ №2
(в форме контрольной работы)

по дисциплине «Информационная безопасность»

1. Регламентация относится к _____ методам защиты информации.
а) законодательным
б) организационным
в) аппаратным

2. Препятствие относится к _____ методам защиты информации.
а) физическим
б) организационным
в) аппаратным

3. Маскировка относится к _____ методам защиты информации.
а) программным
б) аппаратным
в) физическим

4. Электронно-цифровая подпись позволяет ...
а) удостовериться в истинности отправителя и целостности сообщения
б) зашифровать сообщение для сохранения его секретности
в) пересылать сообщение по секретному каналу
г) восстанавливать поврежденные сообщения

5. Дайте определение понятия «Надежная система»
а) надежной называется система, эффективно использующая аппаратные и программные средства для обнаружения и предотвращения возможных атак на информацию
б) надежной называется система, использующая достаточные программные и аппаратные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей

без нарушения прав доступа

в) надежной называется система, гарантированность безопасного хранения информации в которой близка к 100%

6. Что из перечисленного относится к числу основных аспектов информационной безопасности:

а) подотчетность

б) приватность

в) конфиденциальность

7. Что не является традиционным направлением защиты компьютерной информации

а) криптография

б) антивирусология

в) линейное программирование

г) защита от несанкционированного копирования

д) сетевая защита

8. Что является объектом защиты информации?

а) компьютерная система или автоматизированная система обработки данных (АСОД)

б) вычислительные сети

в) системы управления базами данных (СУБД)

г) память ЭВМ

9. Что является предметом защиты в компьютерных системах?

а) электронные и электромеханические устройства, а также машинные носители

б) информация

в) системы передачи данных (СПД)

10. Утечка информации – это …

а) несанкционированный процесс переноса информации от источника к злоумышленнику

б) процесс раскрытия секретной информации

в) процесс уничтожения информации

г) непреднамеренная утрата носителя информации

11. Основные угрозы конфиденциальности информации:

а) переадресовка

б) перехват данных

в) блокирование

г) злоупотребления полномочиями

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

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

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

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

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

а) несанкционированного управления удаленным компьютером

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

в) перехвата или подмены данных на путях транспортировки

г) поставки неприемлемого содержания

14. Причины возникновения ошибки в данных

а) Погрешность измерений

б) Ошибка при записи результатов измерений в промежуточный документ

в) Неверная интерпретация данных

г) Ошибки при переносе данных с промежуточного документа в компьютер

д) Использование недопустимых методов анализа данных

е) Неустранимые причины природного характера

ж) Преднамеренное искажение данных

з) Ошибки при идентификации объекта или субъекта хозяйственной деятельности

15. Сколько типов архитектуры используется при создании системы сертификации в инфраструктуре с открытыми ключами?

а) один

б) два

в) три

г) четыре

16. Какой цифровой документ подтверждает соответствие между открытым ключом и информацией, идентифицирующей владельца ключа?

а) код пользователя.

б) цифровой сертификат

в) доверенность

г) шифр программы

17. Как следует понимать термин «аутентификация»?

а) задание формата цифрового сертификата
б) название одного из механизмов защиты информации
в) подтверждение цифровой подписи
г) проверка подлинности идентификации пользователей

18. Сколько существует механизмов реализации защитных функций?
а) 1
б) 2
в) 3
г) 4

19. Сколько уровней возможностей существует для нарушителей средств защиты информации автоматизированных систем?
а) 1
б) 2
в) 3
г) 4

20. Шифры с секретным ключом – это:
а) симметричная схема
б) асимметричная схема

21. Асимметричная схема шифрования предполагает наличие:
а) секретного ключа
б) открытого ключа

22. Наличие секретного ключа позволяет:
а) зашифровать сообщение
б) расшифровать сообщение
в) зашифровать и расшифровать сообщение

23. Методы _____ позволяют скрыть не только смысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации.
а) шифрования
б) стеганографии
в) кодирования
г) сжатия

24. Какие преобразования шифра выполняются при операции рассеивания?
а) сжатие шифра
б) передача текста небольшими частями
в) наложение ложных сообщений
г) изменение любого знака открытого текста или ключа

25. Какие шифры называются послойными?

а) состоящие из слоев шифрования

б) состоящие из цепочки циклов шифрования

в) выполняющие единственное преобразование информационного сообщения.

г) обеспечивающие высокоэффективное шифрование

26. Одинаковые ключи для шифрования и дешифрования имеет _____ криптология.

а) симметричная

б) асимметричная

в) двоичная

27. Как работают поточные криптосистемы?

а) текст сообщения разбиваетсяна отдельные потоки и затем осуществляют преобразование этих потоков с использованием ключа

б) текст сообщения разбиваетсяна отдельные блоки и затем осуществляют преобразование этих блоков с использованием ключа

в) на основе ключа системы вырабатывается некая последовательность - так называемая выходная гамма, которая затем накладывается на текст сообщения

г) вырабатывается случайная последовательность символов, которая затем накладывается на текст сообщения

28. Дайте определение понятия криптография:

а) Криптография – это наука о защите информации от несанкционированного доступа посторонними лицами

б) Криптография – наука о защите информации от прочтения её посторонними лицами, достигаемая путем шифрования, которое делает защищенные данные труднораскрываемыми без знания специальной (ключевой) информации

в) Криптография – это наука о защите информации с помощью математических преобразований, которые являются симметричными

29. Дайте определение понятия шифр:

а) Шифр – это совокупность преобразований, с помощью которых осуществляется кодирование информации

б) Шифр – это алгоритм преобразования, в котором используется ключ

в) Шифр – это совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом преобразования

30. Модификациями шифра Цезаря являются следующие системы шифрования:

а) Шифр Хилла
б) Тюремный шифр
в) Книжный шифр
г) Шифр Диффи-Хелмана
д) Шифр Плэйфер
е) Шифр Гронсфельда

Критерии оценки:
Студент аттестован, если правильно ответил более чем на 15 вопросов.