Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Кубанский государственный университет»
в г. Армавире

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.03 «Информационная безопасность»

Направление подготовки: 38.03.05 Бизнес-информатика
Направленность (профиль): Электронный бизнес
Форма обучения: Очная

Квалификация (степень) выпускника: Бакалавр

Программа подготовки: академическая

Краснодар 2016

Рабочая программа дисциплины «Информационная безопасность» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 38.03.05 Бизнес информатика

Программу составил:
Алексанян Г.А., канд. пед. наук, ст. преп., кафедры экономики и менеджмента

Рабочая программа обсуждена на заседании кафедры экономики и менеджмента
протокол № 1 «27» августа 2018г.

Заведующий кафедрой Косенко С.Г.

Утверждена на заседании учебно-методической комиссии филиала
Протокол № 1 «27» августа 2018 г.

Председатель УМК Кабачевская Е.А.

Рецензенты:

Дегтярева Е.А., канд. пед. наук, доцент, кафедры социально-гуманитарных дисциплин филиала ФГБОУ ВПО «Кубанский государственный университет» в г. Тихорецке

Горовенко Л.А. зав. кафедрой ОНД АМТИ, канд.тех.наук

Лист изменений к рабочей программе учебной дисциплины

«Информационная безопасность»

Содержание изменений	№ протокола заседания кафедры, дата	ФИО / подпись зав. кафедрой
В соответствии с выходом нового приказа от 05.04.2017 №301 «Об утверждении Порядка организации и осуществлении образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры» была изменена рабочая программа	№1 от 28.08.2017	

Лист изменений к рабочей программе учебной дисциплины

	ФИО, подпись зав. кафедрой
На основании решения учёного совета КубГУ от 27.04.2018 года, протокол № 9, в связи с реорганизацией структуры филиала ФГБОУ ВО «КубГУ» в г.Армавире с 01.08.2018 года Кафедра «математики и информатики» присоединена к Кафедре «социально-гуманитарных дисциплин» и переименована в кафедру «гуманитарных и естественнонаучных дисциплин» (Приказ № 855 от 11.05.2018 г «О реорганизации структуры филиала ФГБОУ ВО «КубГУ» в г.Армавире) Выпускающей кафедрой для направления подготовки 38.03.05 Бизнес-информатика является кафедра экономики и менеджмента. В связи с этим произведена актуализация рабочих программ дисциплин, программ практик, программы ГИА и фондов оценочных средств	

1 Цели и задачи изучения дисциплины

1.1 Цель освоения дисциплины

Основной целью изучения дисциплины «Информационная безопасность» является формирование у обучающихся глубокого понимания и приобретения знаний, необходимых в области информационной безопасности.

1.2 Задачи дисциплины:

- формирование общего представления о современных концепциях информационной безопасности;
-знакомство с различными методами защиты информации от несанкционированного доступа;
-изучение криптографических средств, как основного инструмента обеспечения сохранности компьютерной информации;
-приобретение практических навыков работы с современными аппаратными и программными средствами защиты информации.

1.3 Место дисциплины в структуре образовательной программы.

Дисциплина «Информационная безопасность» относится к вариативной части Блок 1. «Дисциплины (модули)» учебного плана.

1.4 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы.

Изучение данной учебной дисциплины направлено на формирование у обучающихся общепрофессиональных/профессиональных компетенций (*ОПК/ПК)*

№ п.п.	Индекс компетенции	Содержание компетенции	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
1	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	основные понятия информационной безопасности, основные принципы организации и алгоритмы функционирования систем безопасности в современных операционных системах и оболочках;	решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	методами оценки защищённости систем с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;
2	ПК-9	организация взаимодействия с	основы информационн	взаимодействовать с клиентами и	приемами взаимодействи

		клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия	ой безопасности ИТ-инфраструктуры предприятия;	партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия;	я с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия;
3	ПК-11	умение защищать права на интеллектуальную собственность	основополагающие категории интеллектуальной собственности, правовые понятия и термины в их взаимосвязи;	использовать информационные технологии и системы для эффективного взаимодействия с обладателем прав на объект интеллектуальной собственности;	навыками использования возможностей наиболее распространенных классификаторов, баз данных интеллектуальной собственности, прикладных программных средств общего и специального назначений, локальных вычислительных сетей, глобальной сети Internet для практического решения задач по коммерциализации интеллектуальной собственности; навыками поиска необходимых нормативных актов.
4	ПК-21	умение консультировать заказчиков по вопросам совершенствовани	технологии защиты информации и алгоритмы традиционных	консультировать заказчиков по вопросам совершенствования	методами и средствами технической защиты информации

		я управления информационной безопасностью ИТ-инфраструктуры предприятия	методов шифрования данных.	управления информационной безопасностью ИТ-инфраструктуры предприятия;	

2. Структура и содержание дисциплины.

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 3 зач.ед. (108 часов), их распределение по видам работ представлено в таблице

(для студентов ОФО).

Вид учебной работы		Всего часов	Семестры (часы)				
			1	2	3	4	5
Контактная работа, в том числе:		**55,3**					**55,3**
Аудиторные занятия (всего):		52,3	-	-	-	-	52,3
Занятия лекционного типа		18	-	-	-	-	18
Занятия семинарского типа (семинары, практические занятия)		34	-	-	-	-	34
Лабораторные занятия		-	-	-	-	-	-
Иная контрольная работа:		**3,3**					**3,3**
Контроль самостоятельной работы (КСР)		3					3
Промежуточная аттестация (ИКР)		0,3					0,3
Самостоятельная работа, в том числе:		**17**					**17**
Курсовая работа		-	-	-	-	-	-
Проработка учебного (теоретического) материала		4	-	-	-	-	4
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		4	-	-	-	-	4
Реферат		4	-	-	-	-	4
Подготовка к текущему контролю		5	-	-	-	-	5
Контроль:							
Подготовка к экзамену		**35,7**					35,7
Общая трудоемкость	**час.**	**108**	**-**	**-**	**-**	**-**	**108**
	в том числе контактная работа	**55,3**					**55,3**
	зач. ед	**3**					**3**

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в 5 семестре *(очная форма)*

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС

1	2	3	4	5	6	7
1.	Основные понятия информационной безопасности и защиты информации	7	1	2		2
2.	Требования, предъявляемые к защите информации	9	1	2		2
3.	Аспекты информационной безопасности	6	1	2		2
4.	Угрозы. Основные понятия и определения	9	2	4		2
5.	Вероятностная модель расчета уязвимости информации	6	1	2		2
6.	Вероятностная модель расчета уязвимости информации	6	1	2		2
7.	Защита от утечки по акустическим каналам	6	1	2		2
8.	Защита от утечки по электромагнитным каналам	7	1	2		2
9.	Защита от утечки по материально-вещественным каналам	6	1	2		1
10.	Методы определения требований к защите информации. Множество задач защиты информации.	6	1	2		
11.	Классификация способов и средств защиты информации. Технические средства.	9	2	4		
12.	Вредоносное программное обеспечение	10	2	2		
13.	Вирусы	11	1	4		
14.	Антивирусные средства.	10	2	2		
	КСР	3				
	ИКР	0,3				
	Контроль	35,7				
	Итого по дисциплине:	**108**	**18**	**34**	**-**	**17**

Примечание: Л – лекции, ПЗ – практические занятия / семинары, ЛР – лабораторные занятия, СРС – самостоятельная работа студента

2.3 Содержание разделов дисциплины:

2.3.1 Занятия лекционного типа

№ раздела	Наименование темы	Содержание раздела	Форма текущего контроля
1	2	3	4
1	Основные понятия информационной безопасности и защиты информации	**Тема 1.** Информационная безопасность. 1.Понятие информации, информации безопасности, защиты информации. 2.Общие концептуальные положения информационной безопасности.	Реферат (Р)
2	Требования, предъявляемые к защите информации	**Тема 2.** Защита информации. 1.Требование к системам общего пользования. 2. Мероприятия по обеспечению защиты в системах общего пользования	Реферат (Р)

3	Аспекты информационной безопасности	**Тема 3.** Доступность, целостность и конфиденциальность информационной безопасности.	Реферат (Р)
4	Угрозы. Основные понятия и определения	**Тема 4.** Угрозы. 1.Понятие угрозы. 2.Системная классификация угроз.	Реферат (Р)
5	Вероятностная модель расчета уязвимости информации	**Тема 5.** Уязвимость информации. 1.Взаимодействие параметров угроз информации. 2.Безопасность в базах данных.	Реферат (Р)
6	Вероятностная модель расчета уязвимости информации	**Тема 6.** Каналы утечки информации. 1. Классификация каналов утечки информации. 2.Источники образования каналов утечки.	Реферат (Р)
7	Защита от утечки по акустическим каналам	**Тема 7.** Защита информации от угроз. 1.Сущность оценки угроз информации. 2.Задачи оценки угроз информации.	Реферат (Р)
8	Защита от утечки по электромагнитным каналам	**Тема 8.** Анализ уязвимости. 1. Модель нарушителей. 2. Особо важные зоны.	Реферат (Р)
9	Защита от утечки по материально-вещественным каналам	**Тема 9.** Декомпозиция компонента информационной системы. 1. Оценка базовой уязвимости.	Реферат (Р)
10	Методы определения требований к защите информации. Множество задач защиты информации.	**Тема 10.** Задачи, возникающие при определении требований к защите информации. 1. Оценка параметров. 2. Классификация информации по важности.	Реферат (Р)
11	Классификация способов и средств защиты информации. Технические средства.	**Тема 11.** Способы защиты информации. 1. Средства защиты от речевой информации. 2. Методы поиска электронных устройств перехвата информации.	Реферат (Р)
12	Вредоносное программное обеспечение	**Тема 12.** Классификация вредоносного программного обеспечения. 1. Программные закладки. 2.Ловушка, люк, червь, троянский конь, бомба.	Реферат (Р)

13	Вирусы	**Тема 13.** Общее представление о вирусах. 1. Этапы функционирования. 2. Классификация вирусов.	Реферат (Р)
14	Антивирусные средства.	**Тема 14.** Виды антивирусных средств. 1. Классификация антивирусных программных средств. 2.Детекторы, полифаги, ревизоры, сторожа, вакцины.	Реферат (Р)

В данном подразделе приводится описание содержания дисциплины, структурированное по разделам, с указанием по каждому разделу формы текущего контроля: У.о. – устный опрос, П.о. – письменный опрос; Р-реферат.

2.3.2 Занятия семинарского типа.

№ раздела	Наименование темы	Содержание раздела	Форма текущего контроля
1	Основные понятия информационной безопасности и защиты информации	**Тема 1.** Понятие информации, информации безопасности, защиты информации. 1. Общие концептуальные положения информационной безопасности. 2. Доктрина РФ в области информационной безопасности и защиты данных. 3. Изучение основных документов РФ в области информационной безопасности.	Тестирование (Т)
2	Требования, предъявляемые к защите информации	**Тема 2.** Требование к системам общего пользования. 1. Мероприятия по обеспечению защиты в системах общего пользования. 2. Политика и программа безопасности. 3. Составление программы безопасности на 1, 2 и 3 уровнях. 4. Синхронизация программы безопасности с жизненным циклом информационной системы.	Тестирование (Т) Дискуссия (Д)
3	Аспекты информационной безопасности	**Тема 3.** Доступность, целостность и конфиденциальность информационной безопасности.	Тестирование (Т)
4	Угрозы. Основные понятия и определения	**Тема 4.** Понятие угрозы. 1. Системная классификация угроз. 2. Определение угроз безопасности по отраслям.	Тестирование (Т), устный опрос (Уо)

5	Вероятностная модель расчета уязвимости информации	**Тема 5.** Взаимодействие параметров угроз информации. 1. Безопасность в базах данных.	Тестирование (Т)
6	Вероятностная модель расчета уязвимости информации	**Тема 6.** Каналы утечки информации. 1. Классификация каналов утечки информации. 2. Источники образования каналов утечки.	Тестирование (Т)
7	Защита от утечки по акустическим каналам	**Тема 7.** Сущность оценки угроз информации. 1. Задачи оценки угроз информации.	Тестирование (Т), устный опрос (Уо)
8	Защита от утечки по электромагнитным каналам	**Тема 8.** Анализ уязвимости. 1. Модель нарушителей. 2.Особо важные зоны.	Тестирование (Т), устный опрос (Уо)
9	Защита от утечки по материально-вещественным каналам	**Тема 9.** Декомпозиция компонента информационной системы. 1. Оценка базовой уязвимости.	Тестирование (Т)
10	Методы определения требований к защите информации. Множество задач защиты информации.	**Тема 10.** Задачи, возникающие при определении требований к защите информации. 1. Оценка параметров. 2. Классификация информации по важности.	Тестирование (Т), устный опрос (Уо)
11	Классификация способов и средств защиты информации. Технические средства.	**Тема 11.** Средства защиты от речевой информации. 1. Методы поиска электронных устройств перехвата информации. 2. Установка и настройка программных средств защиты данных.	Тестирование (Т), устный опрос (Уо)
12	Вредоносное программное обеспечение	**Тема 12.** Классификация вредоносного программного обеспечения. 1. Программные закладки. 2.Ловушка, люк, червь, троянский конь, бомба.	Тестирование (Т), устный опрос (Уо)
13	Вирусы	**Тема 13.** Общее представление о вирусах. 1. Этапы функционирования. 2. Классификация вирусов. 3.Выявление и классификация вирусов.	Тестирование (Т), устный опрос (Уо)
14	Антивирусные средства.	**Тема 14.** Классификация антивирусных программных	Тестирование (Т), устный опрос (Уо)

		средств. 1. Детекторы, полифаги, ревизоры, сторожа, вакцины. 2. Установка и настройка антивирусного программного обеспечения.	

2.3.3 Лабораторные занятия.

Лабораторные занятия тематическим планом не предусмотрены

2.3.4 Примерная тематика курсовых работ

Курсовые работы (проекты) тематическим планом не предусмотрены

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Конспектирование	Методические рекомендации по организации самостоятельной работы обучающихся (рассмотрены и утверждены на заседании кафедры экономики и менеджмента филиала ФГБОУ ВО «КубГУ» в г. Армавире 27 августа 2018 г., протокол №1)
2	Углубленный анализ научно-методической литературы	Методические рекомендации по организации самостоятельной работы обучающихся (рассмотрены и утверждены на заседании кафедры экономики и менеджмента филиала ФГБОУ ВО «КубГУ» в г. Армавире 27 августа 2018 г., протокол №1); - Основная и дополнительная литература по дисциплине.
3	Подготовка рефератов	Методические рекомендации по подготовке, написанию и порядку оформления рефератов (рассмотрены и утверждены на заседании кафедры экономики и менеджмента ФГБОУ ВО «КубГУ» в г. Армавире 27 августа 2018 г., протокол №1)

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

–в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

3. Образовательные технологии.

При реализации учебной работы по дисциплине используются как традиционные образовательные технологии, ориентированные на организацию образовательного процесса, предполагающую прямую трансляцию знаний от преподавателя к обучающемуся, так и активные и интерактивные формы проведения занятий - дискуссия.

Используемые образовательные технологии по-новому реализуют содержание обучения и обеспечивают реализацию компетенций, подразумевая научные подходы к организации образовательного процесса, изменяют и предоставляют новые формы, методы и средства обучения.

Семестр	Вид занятия (ПЗ)	Используемые интерактивные образовательные технологии	Количество часов
5	**ПЗ** – Требования, предъявляемые к защите информации	Дискуссия	2
	Итого:		**2**

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации.

4.1 Фонд оценочных средств для проведения текущего контроля.

Примерные вопросы для устного опроса

Тема 1. Понятие информации, информации безопасности, защиты информации.

1. Общие концептуальные положения информационной безопасности.
2. Доктрина РФ в области информационной безопасности и защиты данных.
3. Изучение основных документов РФ в области информационной безопасности.

Тема 2. Требование к системам общего пользования.

1. Мероприятия по обеспечению защиты в системах общего пользования.
2. Политика и программа безопасности.
3. Составление программы безопасности на 1, 2 и 3 уровнях. 4. Синхронизация программы безопасности с жизненным циклом информационной системы.

Тема 3. Доступность, целостность и конфиденциальность информационной безопасности.

Тема 4. Понятие угрозы.

1. Системная классификация угроз.
2. Определение угроз безопасности по отраслям.

Тема 5. Взаимодействие параметров угроз информации.

1. Безопасность в базах данных.

Тема 6. Каналы утечки информации.

1. Классификация каналов утечки информации.

2. Источники образования каналов утечки.

Тема 7. Сущность оценки угроз информации.

1. Задачи оценки угроз информации.

Тема 8. Анализ уязвимости.

1. Модель нарушителей.

2.Особо важные зоны.

Тема 9. Декомпозиция компонента информационной системы.

1. Оценка базовой уязвимости.

Тема 10. Задачи, возникающие при определении требований к защите информации.

1. Оценка параметров.

2. Классификация информации по важности.

Тема 11. Средства защиты от речевой информации.

1. Методы поиска электронных устройств перехвата информации. 2. Установка и настройка программных средств защиты данных.

Тема 12. Классификация вредоносного программного обеспечения.

1. Программные закладки.

2.Ловушка, люк, червь, троянский конь, бомба.

Тема 13. Общее представление о вирусах.

1. Этапы функционирования.

2. Классификация вирусов.

3.Выявление и классификация вирусов.

Тема 14. Классификация антивирусных программных средств.

1. Детекторы, полифаги, ревизоры, сторожа, вакцины.

2. Установка и настройка антивирусного программного обеспечения.

Примерные варианты тестовых заданий

1. Задание

Выбери правильный ответ

На чем основан принцип работы антивирусных мониторов?

- На перехватывании вирусоопасных ситуаций и сообщении об этом пользователю
- На проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются маски
- На подсчете контрольных сумм для присутствующих на диске файлов или системных секторов. Эти суммы затем сохраняются в базе данных антивируса, а также другая информация: длина файлов, дата их последней модификации и т.д.
- На защите системы от поражения вирусом какого-то определенного вида. Файлы на дисках модифицируются таким образом, что вирус принимает их за уже зараженные

2. Задание

Выбери правильный ответ

На чем основан принцип работы антивирусных иммунизаторов?

- На защите системы от поражения вирусом какого-то определенного вида. Файлы на дисках модифицируются таким образом, что вирус принимает их за уже зараженные
- На проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются маски
- На подсчете контрольных сумм для присутствующих на диске файлов или

системных секторов. Эти суммы затем сохраняются в базе данных антивируса, а также другая информация: длина файлов, дата их последней модификации и т.д.

3. Задание

Выбери правильный ответ

Что необходимо сделать при обнаружении файлового вируса?

- Компьютер необходимо отключить от сети и проинформировать системного администратора
- Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются
- вместо отключения компьютера от сети достаточно на период лечения убедиться в том, что соответствующий редактор неактивен

4. Задание

Выбери правильный ответ

Что необходимо сделать при обнаружении загрузочного вируса?

- Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются
- Компьютер необходимо отключить от сети и проинформировать системного администратора
- Вместо отключения компьютера от сети достаточно на период лечения убедиться в том, что соответствующий редактор неактивен

5. Задание

Выбери правильный ответ

Что необходимо сделать при обнаружении макровируса?

- Вместо отключения компьютера от сети достаточно на период лечения убедиться в том, что соответствующий редактор неактивен
- Компьютер необходимо отключить от сети и проинформиравать системного администратора
- Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются

6. Задание

Выбери правильный ответ

В чем заключается метод защиты - ограничение доступа?

- В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям
- В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями
- В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы
- В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. приведении её к неявному виду

7. Задание

Выбери правильный ответ

В чем заключается метод защиты информации - разграничение доступа?

- В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями

- В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям
- В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы
- В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении её к неявному виду

8. Задание

Выбери правильный ответ

В чем заключается метод защиты информации - разделение доступа (привилегий)

- В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы
- В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям
- В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями
- В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении её к неявному виду

9. Задание

Выбери правильный ответ

В чем заключается криптографическое преобразование информации?

- В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении её к неявному виду
- В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям
- В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями
- В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы

Информационная безопасность в условиях функционирования в России глобальных сетей

10. Задание

Ответить на вопрос

Что означает термин БЕЗОПАСНОСТЬ ИНФОРМАЦИИ

- Потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному её тиражированию
- Свойство системы, в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.
- Защищенность информации от нежелательного её разглашения, искажения, утраты или снижения степени доступности информации, а также незаконного её тиражирования

11. Задание

Ответить на вопрос

Кто является хакером?

- Это лица, проявляющие чрезмерный интерес к устройству сложных систем и обладающие большими познаниями по части архитектуры и принципов устройства вычислительной среды или технологии телекоммуникаций, что используется для похищения информации
- Это лица, изучающие систему с целью её взлома. Они реализуют свои криминальные наклонности в похищении информации и написании разрушающего программного обеспечения и вирусов, используют принципы построения протоколов сетевого обмена
- Это лица, которые "взламывая" интрасети, получают информацию о топологии этих сетей, используемых в них программно-аппаратных средствах и информационных ресурсах. Эти сведения они продают заинтересованным лицам

12. Задание

Выбери правильный ответ

Кто является кракером?

- Это лица, изучающие систему с целью её взлома. Они реализуют свои криминальные наклонности в похищении информации и написании разрушающего программного обеспечения и вирусов, при этом применяют различные способы атак на компьютерную систему, используя при
- Это лица, проявляющие чрезмерный интерес к устройству сложных систем, обладающие большими познаниями по части архитектуры и принципов устройства вычислительной среды, что используется для похищения информации
- Это лица, которые "взламывая " интрасети", получают информацию о топологии этих сетей, используемых в них программно-аппаратных средствах и информационных ресурсах. Эти сведения они продают заинтересованным лицам

13. Задание

Выбери правильный ответ

Кто является фракером?

- Это лица, которые "взламывая" интрасети, получают информацию о топологии этих сетей, используемых в них программно-аппаратных средствах. Эти сведения они продают заинтересованным лицам.
- Это лица, проявляющие чрезмерный интерес к устройству сложных систем, обладающие большими познаниями по части архитектуры и принципов устройства вычислительной среды
- Это лица, изучающие систему с целью её взлома. Они реализуют свои криминальные наклонности в похищении информации и разрушающего программного обеспечения и вирусов

14. Задание

Выбери правильный ответ

Что означает термин ДОСТУПНОСТЬ ИНФОРМАЦИИ?

- Это свойство системы, в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия
- Это подверженность информации воздействию различных дестабилизирующих факторов, которые могут привести к нарушению её конфиденциальности, целостности, доступности, или неправомерному её тиражированию
- Это свойство информации, заключающееся в её существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному её состоянию)

15. Задание

Выбрать правильный ответ

Что означает термин ЦЕЛОСТНОСТЬ ИНФОРМАЦИИ?

- Это свойство информации, заключающееся в её существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному её состоянию)
- Это свойство системы, в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия
- Это подверженность информации воздействию различных дестабилизирующих факторов, которые могут привести к нарушению её конфиденциальности, целостности, доступности, или неправомерному её тиражированию

16. Задание

Выбери правильный ответ

Что означает термин УЯЗВИМОСТЬ ИНФОРМАЦИИ?

- Это подверженность информации воздействию различных дестабилизирующих факторов, которые могут привести к нарушению её конфиденциальности, целостности, доступности, или неправомерному её тиражированию
- Это свойство системы, в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия
- Это свойство информации, заключающееся в её существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному её состоянию)

17. Задание

Выбери правильный ответ

В чем заключается конфиденциальность компонента системы?

- В том, что он доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия
- В том, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права
- В том, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы

18. Задание

Выбери правильный ответ

В чем заключается целостность компонента системы?

- В том, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права
- В том, что он доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия
- В том, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы

19. Задание

Выбери правильный ответ

В чем заключается доступность компонента системы?

- В том, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы
- В том, что он доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия
- В том, что он может быть модифицирован только субъектом, имеющим для этого

соответствующие права

20. Задание

Выбери правильный ответ

Что означает термин ПРАВОВЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ?

- Это действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения
- Это традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией
- Это меры, регламентирующие процессы функционирования системы обработки данных, использования её ресурсов

21. Задание

Выбери правильный ответ

Что означает термин МОРАЛЬНО-ЭТИЧЕСКИЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ?

- Это традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией
- Это действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения
- Это меры, регламентирующие процессы функционирования системы обработки данных, использование её ресурсов

22. Задание

Выбери правильный ответ

Что означает термин ОРГАНИЗАЦИОННЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ?

- Это меры, регламентирующие процессы функционирования системы обработки данных, использование её ресурсов, деятельность персонала, а так же порядок взаимодействия пользователей с системой
- Это действующие в стране законы, указы и другие нормативные акты
- Это традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией

23. Задание

Выбери правильный ответ

Что означает термин ФИЗИЧЕСКИЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ?

- Это разного рода механические или электронно-механические устройства и сооружения, специально предназначенные для создания различных препятствий на возможных путях проникновения доступа потенциальных нарушителей к компонентам защищаемой информации
- Это действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения
- Это меры, регламентирующие процессы функционирования системы обработки данных, использование её ресурсов

24. Задание

Выбери правильный ответ

Что означает термин АУТЕНТИФИКАЦИЯ?

- Это проверка подлинности объекта или субъекта
- Это проверка целостности информации, программы, документа
- Это присвоение имени субъекту или объекту

25. Задание

Выбери правильный ответ
Что означает термин ВЕРИФИКАЦИЯ?

- Это проверка целостности информации, программы, документа
- Это проверка подлинности субъекта или объекта
- Это присвоение имени субъекту или объекту

26. Задание

Выбери правильный ответ
Что означает термин ИДЕНТИФИКАЦИЯ?

- Это присвоение имени субъекту или объекту
- Это проверка подлинности субъекта или объекта
- Это проверка целостности информации, программы, документа

27. Задание

Выбери правильный ответ
Что означает термин КРИПТОГРАФИЯ?

- Это метод специального преобразования информации с целью сокрытия от посторонних лиц
- Это преобразование информации в виде условных сигналов с целью автоматизации её хранения, обработки, передачи и ввода-вывода
- Это криптографическое преобразование информации приеё передаче по каналам связи от одного элемента вычислительной сети к другому

28. Задание

Выбери правильный ответ
Что означает термин КОДИРОВАНИЕ ИНФОРМАЦИИ?

- Это преобразование информации в виде условных сигналов с целью автоматизации её хранения, обработки, передачи и ввода-вывода
- Это метод специального преобразования информации с целью сокрытия от посторонних лиц
- Это криптографическое преобразование информации при её передаче по каналам связи от одного элемента в вычислительной сети к другому

29. Задание

Выбери правильный ответ
Что означает термин ЛИНЕЙНОЕ ШИФРОВАНИЕ?

- Это криптографическое преобразование информации при её передаче по каналам связи от одного элемента вычислительной сети к другому
- Это метод специального преобразования информации с целью сокрытия от посторонних лиц
- Это преобразование информации в виде условных сигналов с целью автоматизации её хранения, обработки, передачи и ввода-вывода

30. Задание

Выбери правильный ответ
Как классифицируются виды угроз информации по природе возникновения?

- Стихийные бедствия, несчастные случаи, ошибки обслуживающего персонала и пользователей, злоупотребления обслуживающего персонала и пользователей, злоумышленные действия нарушителей, сбои и отказы оборудования
- Угрозы персоналу, информации, информационным системам, материальным, финансовым, информационным данным
- Угрозы информационным системам, материальным, финансовым, информационным данным, злоумышленные действия нарушителей, сбои и отказы оборудования

31. Задание

Выбери правильный ответ

Как классифицируются виды угроз информации по ориентации на ресурсы?

- Угрозы персоналу, информации, информационным системам, материальным, финансовым, информационным данным
- Стихийные бедствия, несчастные случаи, ошибки обслуживающего персонала и пользователей, злоупотребления обслуживающего персонала и пользователей, злоумышленные действия нарушителей, сбои и отказы оборудования
- Угрозы информационным системам, материальным, финансовым, информационным данным, злоумышленные действия нарушителей, сбои и отказы оборудования

32. Задание

Выбери правильный ответ

Какие угрозы относятся к естественным?

- Отказы и сбои аппаратуры; Помехи на линиях связи от воздействий внешней среды; аварийные ситуации; стихийные бедствия
- Ошибки человека как звена системы; схемные и системотехнические ошибки разработчиков структурные, алгоритмические и программные ошибки; действия человека, направленные на несанкционированные воздействия на информацию
- Аварийные ситуации; стихийные бедствия; ошибки человека как звена системы; схемные и системотехнические ошибки разработчиков

33. Задание

Выбери правильный ответ

Какие угрозы информации относятся к искусственным?

- Ошибки человека как звена системы; схемные и системотехнические ошибки разработчиков; структурные, алгоритмические и программные ошибки; действия человека, направленные на несанкционированные воздействия на информацию
- Отказы и сбои аппаратуры; помехи на линиях связи от воздействий внешней среды; аварийные ситуации; стихийные бедствия
- Аварийные ситуации; стихийные бедствия; ошибки человека как звена системы; схемные и системотехнические ошибки разработчиков

34. Задание

Выбери правильный ответ

Какие угрозы информации относятся к случайным?

- Проявление ошибок программно-аппаратных средств АС; некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности; неумышленная порча носителей информации
- Несанкционированное чтение информации; несанкционированное изменение информации; несанкционированное уничтожение информации; полное или частичное разрушение операционной системы
- Пересылка данных по ошибочному адресу абонента; ввод ошибочных данных; несанкционированное уничтожение информации; полное или частичное разрушение операционной системы

35. Задание

Выбери правильный ответ

Какие угрозы информации относятся к преднамеренным?

- Несанкционированное чтение информации; несанкционированное изменение информации; несанкционированное уничтожение информации; полное или частичное разрушение операционной системы
- Проявление ошибок программно-аппаратных средств АС; некомпетентное

использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности; неправомерное включение оборудования или изменение режимов работы устройств и программ
- Пересылка данных по ошибочному адресу абонента; ввод ошибочных данных; несанкционированное уничтожение информации; полное или частичное разрушение операционной системы

Понятие и классификация компьютерных вирусов. Виды противников или «нарушителей»

36. Задание

Выбери правильный ответ

Какими основными свойствами обладает компьютерный вирус?

- Способностью к созданию собственных копий; наличием механизма, обеспечивающего внедрение создаваемых копий в исполняемые объекты вычислительной системы
- Способностью к созданию собственных копий; способностью уничтожать информацию на дисках; способностью создавать всевозможные видео и звуковые эффекты
- Наличием механизма, обеспечивающего внедрение создаваемых копий в исполняемые объекты вычислительной системы; способностью оставлять в оперативной памяти свою резидентную часть; способностью вируса полностью или частично скрыть себя в системе

37. Задание

Выбери правильный ответ

Как классифицируются вирусы в зависимости от среды обитания?

- Файловые; загрузочные; макровирусы; сетевые
- Заражающие DOS, Windows, Win95/NT, OS/2, Word, Excel,Office 97
- Безвредные; неопасные; опасные

38. Задание

Выбери правильный ответ

Как классифицируются вирусы в зависимости от заражаемой ОС?

- Заражающие DOS, Windows, Win95/NT, OS/2, Word, Excel, Office 97.2
- Файловые; загрузочные; макровирусы; сетевые
- Безвредные; неопасные; опасные; очень опасные
- Использование резидентности, использование "стелс"-алгоритмов; использование самошифрование и полиморфичность; использование нестандартных приемов

39. Задание

Выбери правильный ответ

Как классифицируются вирусы в зависимости от особенностей алгоритма работы?

- Использование резидентность; использование "стелс"-алгоритмов; использование самошифрование и полиморфичность; использование нестандартных приемов
- Файловые; загрузочные; макровирусы; сетевые
- Заражающие DOS, Windows, Win95/NT,OS/2,Word, Excel, Office 97
- Безвредные; неопасные; опасные; очень опасные

40. Задание

Выбери правильный ответ

Как классифицируются вирусы в зависимости от деструктивных возможностей?

- Безвредные; неопасные; опасные; очень опасные
- Файловые; загрузочные; макровирусы; сетевые
- Заражающие DOS, Windows, Win95/NT,OS/2, Word, Excel, Office 97.4

- Использование резидентность; использование "стелс"-алгоритмов; использование самошифрование и полиморфичность; использование нестандартных приемов

41. Задание

Выбери правильный ответ

В чем заключается принцип работы файлового вируса?

- Вирусы либо различными способами внедряются в выполняемые файлы, либо создают файлы-двойники, либо используют особенности организации файловой системы
- Записывают себя либо в загрузочный сектор диска, либо в сектор, содержащий системный загрузчик винчестера, либо меняют указатель на активный boot-сектор
- Вирусы заражают файлы-документы и электронные таблицы популярных редакторов
- Вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты

42. Задание

Выбери правильный ответ

В чем заключается принцип работы загрузочного вируса?

- Вирусы записывают себя либо в загрузочный сектор диска, либо в сектор, содержащий системный загрузчик винчестера, либо меняет указатель на активный boot-сектор
- Вирусы либо различными способами внедряются в выполняемые файлы, либо создают файлы-двойники, либо используют особенности организации файловой системы
- Вирусы заражают файлы-документы и электронные таблицы популярных редакторов
- Вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты

43. Задание

Выбери правильный ответ

Какие программы относятся к программам Конструкторы вирусов?

- Это утилита, предназначенная для изготовления новых компьютерных вирусов. Они позволяют генерировать исходные тексты вирусов (ASM-файлы), объектные модули и/или непосредственно зараженные файлы
- Это программы, наносящие какие-либо разрушительные действия, т.е. в зависимости от определенных условий или при каждом запуске уничтожающие информацию на дисках, приводящие систему к зависанию и т.п.
- Это программы, которые на первый взгляд являются стопроценными вирусами, но неспособны размножаться по причине ошибок. Например, вирус, который при заражении "забывает" поместить в начало файлов команду передачи управления на код вируса
- Главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика

44. Задание

Выбери правильный ответ

Какие программы относятся к программам полиморфик-генераторы?

- Главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика
- Это программы, наносящие какие-либо разрушительные действия, т.е. в зависимости от определенных условий или при каждом запуске уничтожающие информацию на дисках, приводящие систему к зависанию и т.п.

- Это программы, которые на первый взгляд являются стопроцентными вирусами, но неспособны размножаться по причине ошибок. Например, вирус, который при заражении "забывает" поместить в начало файлов команду передачи управления на код вируса
- Это утилита, предназначенная для изготовления новых компьютерных вирусов. Они позволяют генерировать исходные тексты вирусов (ASM-файлы), объектные модули и/или непосредственно зараженные файлы

45. Задание

Выбери правильный ответ

В чем заключается принцип работы макровируса?

- Вирусы заражают файлы-документы и электронные таблицы популярных редакторов
- Вирусы либо различными способами внедряются в выполняемые файлы, либо создают файлы-двойники, либо используют особенности организации файловой системы
- Вирусы записывают себя либо в загрузочный сектор диска, либо в сектор, содержащий системный загрузчик винчестера, либо меняют указатель на активный boot-сектор
- Вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты

46. Задание

Выбери правильный ответ

В чем заключается принцип работы сетевого вируса?

- Вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты
- Вирусы либо различными способами внедряются в выполняемые файлы, либо создают файлы-двойники, либо используют особенности организации файловой системы
- Вирусы записывают себя либо в загрузочний сектор диска, либо в сектор, содержащий системный загрузчик винчестера, либо меняют указатель на активный boot-сектор
- Вирусы заражают файлы-документы и электронные таблицы популярных редакторов

47. Задание

Выбери правильный ответ

На чем основан алгоритм работы резедентного вируса?

- Вирус при инфицировании компьютера оставляет в оперативной памяти свою часть, которая затем перехватывает обращения ОС к объектам заражения и внедряется в них. Эти вирусы находятся в памяти и являются активными вплоть до выключения компьютера
- Использование этих алгоритмов позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным алгоритмом является перехват запросов ОС на чтение-запись зараженных объектов и затем вирусы временно лечат их
- Используются для того, чтобы максимально усложнить процедуру обнаружения вируса. Эти вирусы трудно поддаются обнаружению. Два образца не будут иметь ни одного совпадения

48. Задание

Выбери правильный ответ

На чем основан алгоритм работы вируса с использованием "стелс"-алгоритмов?

- Использование этих алгоритмов позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным алгоритмом является перехват запросов ОС на чтение-запись зараженных объектов, затем вирусы временно лечат их
- Вирус при инфицировании оставляет в оперативной памяти свою часть, которая затем перехватывает обращения ОС к объектам заражения и внедряется в них. Эти вирусы находятся в памяти вплоть до выключения компьютера
- Используются для того, чтобы максимально усложнить процедуру обнаружения вируса. Эти вирусы достаточно трудно поддаются обнаружению, они не содержат ни одного постоянного участка кода

49. Задание

Выбери правильный ответ

На чем основан алгоритм работы вируса с использованием самошифрования и полиморфичности?

- Эти вирусы достаточно трудно поддаются обнаружению, они не содержат ни одного постоянного участка кода. В большинстве случаев два образца одного итого же вируса не будут иметь ни одного совпадения
- Вирус оставляет в оперативной памяти свою часть, которая затем перехватывает обращения ОС к объектам заражения и внедряется в них. Эти вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки ОС
- Использование этих алгоритмов позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным является перехват запросов ОС на чтение-запись зараженных объектов, затем вирусы временно лечат их

50. Задание

Выбери правильный ответ

По деструктивным возможностям, как влияют на работу компьютера безвредные вирусы?

- Никак не влияющие на работу компьютера, кроме уменьшения свободной памяти на диске в результате своего распространения
- Влияние ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и прочими эффектами
- Могут привести к серьезным сбоям в работе компьютера
- В алгоритм работы заведомо заложены процедуры, которые могут вызвать потерю программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти

51. Задание

Выбери правильный ответ

По деструктивным возможностям, как влияют на работу компьютера не опасные вирусы?

- Влияние ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и прочими эффектами
- Никак не влияющие на работу компьютера, кроме уменьшения свободной памяти на диске в результате своего распространения
- Могут привести к серьезным сбоям в работе компьютера
- В алгоритм работы заведомо заложены процедуры, которые могут вызвать потерю программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти

52. Задание

Выбери правильный ответ

По диструктивным возможностям, как влияют на работу компьютера опасные вирусы?

- Могут привести к серьезным сбоям в работе компьютера

- Никак не влияющие на работу компьютера, кроме уменьшения свободной памяти на диске в результате своего распространения
- Влияние ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и прочими эффектами
- В алгоритме работы заведомо заложены процедуры, которые могут вызвать потерю программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти

53. Задание

Выбери правильный ответ

По деструктивным возможностям, как влияют на работу компьютера очень опасные вирусы?

- В алгоритм работы заведомо заложены процедуры, которые могут вызвать потерю программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти
- Никак не влияющие на работу компьютера кроме уменьшения свободной памяти на диске в результате своего распространения
- Влияние ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и прочими эффектами

54. Задание

Выбери правильный ответ

По способу заражения файловых вирусов, как работают overwriting-вирусы?

- Вирус не изменяет заражаемых файлов. Алгоритм работы состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, т. е. вирус
- При запуске зараженного файла заставляют ОС выполнить свой код. Этой цели они достигают модификацией необходимых полей файловой системы
- Вирусы никоим образом не связывают свое присутствие с каким-либо выполняемым файлом. При размножении они всего лишь копируют свой код в какие-либо каталоги дисков в надежде, что эти новые копии будут когда-либо запущены пользователем
- Вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое
- Вирус при распространении своих копий обязательно изменяет содержимое файлов, оставляя сами файлы при этом полностью или частично работоспособными

55. Задание

Выбери правильный ответ

По способу заражения файловых вирусов, как работают parasitic-вирусы?

- Вирус при распространении своих копий обязательно изменяет содержимое файлов, оставляя сами файлы при этом полностью или частично работоспособными
- Вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое
- Вирус не изменяет заражаемых файлов. Алгоритм работы состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, т.е. вирус
- Вирусы не изменяют физического содержимого файлов, однако при запуске зараженного файла заставляют ОС выполнить свой код. Этой цели они достигают модификацией необходимых полей файловой системы
- Вирусы никоим образом не связывают свое присутствие с каким-либо

выполняемым файлом. При размножении они всего лишь копируют свой код в какие-либо каталоги дисков в надежде, что эти новые копии будут когда-либо запущены пользователем

56. Задание

Выбери правильный ответ

По способу заражения файловых вирусов, как работают companion-вирусы?

- Вирус не изменяет заражаемых файлов. Алгоритм работы состоим в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, т.е. вирус
- Вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое
- Вирус при распространении своих копий обязательно изменяет содержимое файлов, оставляя сами файлы при этом полностью или частично работоспособными
- Вирусы не изменяют физического содержимого файлов, однако при запуске зараженного файла заставляют ОС выполнить свой код. Этой цели они достигают модификацией необходимых полей файловой системы
- Вирусы никоим образом не связывают свое присутствие с каким-либо выполняемым файлом. При размножении они всего лишь копируют свой код в какие-либо каталоги дисков в надежде, что эти новые копии будут когда-либо запущены пользователем

57. Задание

Выбери правильный ответ

По способу заражения файловых вирусов, как работают link-вирусы?

- Вирусы не изменяют физического содержимого файлов, однако при запуске заражаемого файла заставляет ОС выполнить свой код. Этой цели они достигают модификацией необходимых полей файловой системы
- Вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое
- Вирус при распространении своих копий обязательно изменяет содержимое файлов, оставляя сами файлы при этом полностью или частично работоспособными
- Вирус не изменяет заражаемых файлов. Алгоритм работы состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, т.е. вирус
- Вирусы никоим образом не связывают свое присутствие с каким-либо выполняемым файлом. При размножении они всего лишь копируют свой код в какие-либо каталоги дисков в надежде, что эти новые копии будут когда-либо запущены пользователем

58. Задание

Выбери правильный ответ

По способу заражения файловых вирусов, как работают файловые черви?

- Вирус при распространении своих копий обязательно изменяет содержимое файлов, оставляя сами файлы при этом полностью или частично работоспособными
- Вирус не изменяет заражаемых файлов. Алгоритм работы состоит в том, что для заражаемого файла управление получает именно этот двойник, т.е. вирус
- Вирусы не изменяют физического содержимого файлов, однако при запуске зараженного файла заставляют ОС выполнить свой код. Этой цели они достигают модификацией необходимых полей файловой системы

- Вирусы никоим образом не связывают свое присутствие с каким-либо выполняемым файлом. При размножении они всего лишь копируют свой код в какие-либо каталоги дисков в надежде, что эти новые копии будут когда-либо запущены пользователем
- Вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое

59. Задание

Выбери правильный ответ

Какие программы относятся к программам "Троянские кони" (логические бомбы)

- Это программы, наносящие какие-либо разрушительные действия, т.е. в зависимости от определенных условий или при каждом запуске уничтожающие информацию на дисках, приводящие систему к зависанию и т.п.
- Это программы, которые на первый взгляд являются стопроцентными вирусами, но не способны размножаться по причине ошибок. Например, вирус, который при заражении "забывает" поместить в начало файлов команду передачи управления на код вируса
- Это утилита, предназначенная для изготовления новых компьютерных вирусов. Они позволяют генерировать исходные тексты вирусов (ASM-файлы), объектные модули и/или непосредственно зараженные файлы
- Главной функцией подобного рада программ является шифрование тела вируса и генерация соответствующего расшифровщика

60. Задание

Выбери правильный ответ

Какие программы относятся к программам Intended-вирусы?

- Это программы, которые на первый взгляд являются стопроцентными вирусами, но не способны размножаться по причине ошибок. Например, вирус, который при заражении "забывает" поместить в начало файлов команду передачи управления на код вируса
- Это программы, наносящие какие-либо разрушительные действия, т.е. в зависимости от определенных условий или при каждом запуске уничтожающие информацию на дисках, приводящие систему к зависанию и т.п.
- Это утилита, предназначенная для изготовления новых компьютерных вирусов. Они позволяют генерировать исходные тексты вирусов (ASM-файлы), объектные модули и/или непосредственно зараженные файлы
- Главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика

Примерный перечень тем рефератов

1. Компьютерная преступность в России.
2. Пользователи и злоумышленники сети Internet.
3. Защита от сбоев в электропитании. Источники бесперебойного питания: назначение, характеристики, принципы работы.
4. Защита от формирования электромагнитных полей (излучений). Средства защиты кабельной системы.
5. Средства защиты от сбоев в работе устройств хранения информации.
6. Биометрические средства и технологии установления подлинности.
7. Особенности и проблемы применения биометрических средств защиты информации.
8. Угрозы паролям.
9. Модели разграничения прав доступа.

10. Использование цифровой подписи и хэш-функций.
11. Понятие цифровых сертификатов.
12. Стандарт шифрования AES.
13. Стандарт шифрования RIJNDAEL.
14. Сравнительная характеристика симметричных и ассиметричных методов шифрования.
15. Структура современных компьютерных вирусов.
16. Подробное описание основных классов вирусов.
17. Троянские вирусы.
18. Вирусы - черви.
19. Полиморфные и стелс - вирусы.
20. Политика безопасности антивирусных программ.
21. Сравнительная характеристика антивирусных программ.
22. Политика безопасности брандмауэра.
23. Фильтрация пакетов: достоинства и недостатки.
24. Прокси - серверы.
25 Особенности защиты баз данных.
26. Стандарты защищенности.
27. Угрозы сохранности данных в компьютере случайного характера.
28. Устройства электропитания компьютера, применяемые для защиты компьютера от неблагоприятных воздействий питающей электросети.
29. Криптографическая защита информации (основные понятия).
30. Стандарт шифрования данных DES.

4.2 Фонд оценочных средств для проведения промежуточной аттестации.

Примерный перечень вопросов для подготовки к экзамену

1. Понятие информационной безопасности. Основные составляющие.
2. Основные определения и критерии классификации угроз.
3. Вредоносное программное обеспечение.
4.Основные угрозы целостности. Основные угрозы конфеденциальности.
5.Законодательный уровень информационной безопасности.
6. Обзор российского законодательства в области информационной безопасности.
7. Закон «Об информации, информатизации и защите информации».
8. Закон «О лицензировании отдельных видов деятельности».
9. Обзор зарубежного законодательства в области информационной безопасности.
10. Стандарты и спецификации в области информационной безопасности.
11. Оценочные стандарты и технические спецификации. «Оранжевая книга» как оценочный стандарт.
12. Механизмы безопасности.
13. Классы безопасности.
14. Информационная безопасность распределенных систем. Рекомендации X.800. Сетевые сервисы безопасности.
15. Сетевые механизмы безопасности.
16. Администрирование средств безопасности.
17. О необходимости объектно-ориентированного подхода к информационной безопасности.
18. Основные понятия объектно-ориентированного подхода.
19. Применение объектно-ориентированного подхода к рассмотрению защищаемых систем.

20. Административный уровень информационной безопасности. Основные понятия.

21. Административный уровень информационной безопасности. Политика безопасности.

22. Административный уровень информационной безопасности. Программа безопасности.

23. Административный уровень информационной безопасности. Синхронизация программы безопасности с жизненным циклом систем.

24. Управление рисками. Основные понятия.

25. Подготовительные этапы управления рисками.

26. Основные этапы управления рисками.

27. Процедурный уровень информационной безопасности. Основные классы мер процедурного уровня.

28. Процедурный уровень информационной безопасности. Управление персоналом.

29. Процедурный уровень информационной безопасности. Физическая защита.

30. Процедурный уровень информационной безопасности. Поддержание работоспособности.

31. Процедурный уровень информационной безопасности. Реагирование на нарушение режима безопасности.

32. Процедурный уровень информационной безопасности. Планирование восстановительных работ.

33. Основные понятия программно-технического уровня информационной безопасности.

34. Архитектурная безопасность.

35. Идентификация и аутентификация. Парольная аутентификация.

36. Управление доступом. Ролевое управление доступом.

37. Управление доступом в Java-среде

38. Возможный подход к управлению доступом в распределенной объектной среде.

39. Антивирусные средства.

40. Распространение объектно-ориентированного подхода на информационную безопасность.

41. Понятие угрозы. Наиболее распространенные угрозы. Классификация угроз.

42. Основные нормативные руководящие документы , касающиеся государственной тайны, нормативно-справочные документы.

43. Файловые вирусы.

44. Загрузочные вирусы.

45. Вирусы и операционные системы.

46. Методы и средства борьбы с вирусами.

47. Профилактика заражения вирусами компьютерных систем.

48. Защита информации от случайных угроз.

49. Дублирование информации.

50. Повышение надежности компьютерных систем.

51. Обеспечение отказоустойчивости компьютерных систем.

52. Блокировка ошибочных операций.

53. Защита информации от традиционного шпионажа и диверсий.

54. Система охраны объектов компьютерных систем.

55. Основные понятия шифрования.

56. Методы шифрования с симметричным ключом.

57. Системы шифрования с открытым ключом.

58. Стандарты шифрования.

59. Промышленные программные средства Kerberos, PGP.

60. Методы и средства хранения ключевой информации. Анализ программных реализаций.

Критерии оценки экзамена:

Оценка «отлично» выставляется, если обучающийся свободно владеет материалом, отвечает на основные и дополнительные вопросы билета, выполняет практическое задание.

Оценка «хорошо» выставляется, если обучающийся отвечает на основные вопросы билета, но испытывает некоторые затруднения при ответе на дополнительные вопросы, выполняет практическое задание.

Оценка «удовлетворительно» выставляется обучающемуся, если ответы на основные вопросы билета не достаточно полные и развернутые, возникают некоторые затруднения при выполнении практических заданий.

Оценка «неудовлетворительно» выставляется обучающемуся, если ОПК-1, ПК-9, ПК-11 не освоены, если обучающийся не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями и ошибками решает практические задачи или не в состоянии их решить.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

Образец билета

филиал федерального государственного бюджетного образовательного учреждения высшего образования
«Кубанский государственный университет» в г. Армавире

38.03.05 Бизнес-информатика
Направленность (профиль) – Электронный бизнес
Кафедра экономики и менеджмента

Информационная безопасность

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Распространение объектно-ориентированного подхода на информационную безопасность
2. Основные понятия программно-технического уровня информационной безопасности.

Заведующий кафедрой _____ **С.Г.Косенко**

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

5.1 Основная литература:

1. Артемов А. В. Информационная безопасность [Электронный ресурс]: курс лекций - Орел: МАБИВ, 2014. - 257 с. – URL: http://biblioclub.ru/index.php?page=book_view_red&book_id=428605

2. Прохорова О. В. Информационная безопасность и защита информации [Электронный ресурс]: учебник - Самара: Самарский государственный архитектурно-строительный университет, 2014. - 113 с. – URL: http://biblioclub.ru/index.php?page=book_view_red&book_id=438331

3. Юрьев В. Н. Игровой подход к оценке риска и формированию бюджета информационной безопасности предприятия [Электронный ресурс] учебное пособие: Прикладная Информатика - 2015г. №2: – URL: https://e.lanbook.com/reader/journalArticle/173266/#1

Для освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья имеются издания в электронном виде в электронно-библиотечных системах «Лань» и «Юрайт».

5.2 Дополнительная литература:

1. Информационная безопасность [Электронный ресурс]: учебно-практическое пособие / Башлы П. Н. , Баранова Е. К., Бабаш А. В. - Москва: Евразийский открытый институт, 2011. - 375 с. – URL: http://biblioclub.ru/index.php?page=book_view_red&book_id=90539

2. Гришина, Н.В. Информационная безопасность предприятия [Текст]: уч. пособие для вузов / Н.В. Гришина .- 2-е изд. доп. – М.: Форум , 2015.- 238с

3. Информационная безопасность и защита информации [Электронный ресурс]: сборник студенческих работ, Ответственный редактор: Колябин А.Ю. - Москва: Студенческая наука, 2012. - 1322 с. – URL: http://biblioclub.ru/index.php?page=book_view_red&book_id=227774

5.3. Периодические издания:

1.Информатика и образование
2. Бизнес-информатика

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.

1. ЭБС Издательства «Лань» http://e.lanbook.com/ ООО Издательство «Лань»
2. ЭБС «Университетская библиотека онлайн» www.biblioclub.ru ООО «Директ-Медиа»
3. ЭБС «ZNANIUM.COM» http://www.znanium.com/ ООО «НИЦ ИНФРА-М»
4. ЭБС BOOK.ru http://www.book.ru/ ООО «КноРус медиа»
5. ЭБС «Юрайт» http://www.biblio-online.ru ООО Электронное издательство «Юрайт»

7. Методические указания для обучающихся по освоению дисциплины.

По курсу предусмотрено проведение лекционных занятий, на которых дается основной систематизированный материал. Основной целью лекции является обеспечение теоретической основы обучения, развитие интереса к учебной деятельности и конкретной учебной дисциплине, формирование у обучающихся ориентиров для самостоятельной работы.

Подготовка к практическим занятиям.

Практические занятия ориентированы на работу с учебной и периодической литературой, знакомство с содержанием, принципами и инструментами осуществления и решением основных вопросов теории государства и права, приобретение навыков для самостоятельных оценок результатов оценки государственно-правовых явлений, развития мировой и отечественной правовой мысли. К практическому занятию студент должен ответить на основные контрольные вопросы изучаемой темы, подготовить эссе, решить практико-ориентированные задания и задачи темы, решить кейсы. Кроме того, следует изучить тему по конспекту лекций и учебнику или учебным пособиям из списка литературы.

Тестирование по темам. Подготовка тестированию предполагает изучение материалов лекций, учебной литературы.

Устный опрос. Важнейшие требования к устным ответам студентов – самостоятельность в подборе фактического материала и аналитическом отношении к нему, умение рассматривать примеры и факты во взаимосвязи и взаимообусловленности, отбирать наиболее существенные из них. Ответ обучающегося должно соответствовать требованиям логики: четкое вычленение излагаемой проблемы, ее точная формулировка, неукоснительная последовательность аргументации именно данной проблемы, без неоправданных отступлений от нее в процессе обоснования, безусловная доказательность, непротиворечивость и полнота аргументации, правильное и содержательное использование понятий и терминов.

Написание реферата представляет собой краткое изложение в письменном виде содержания научного труда (трудов), литературы. Это научно-исследовательская работа, в которой студент раскрывает суть изучаемой проблемы, приводит различные точки зрения, а также излагает собственные позиции и взгляды на проблему. Содержание реферата должно быть логичным, а излагаемый материал – носить проблемно-тематический характер.

Дискуссия. Для проведения дискуссии все студенты, присутствующие на практическом занятии, разбиваются на подгруппы, которые обсуждают те или иные вопросы, входящие в тему занятия. Обсуждение может организовываться двояко: либо все подгруппы анализируют один и тот же вопрос, либо какая-то крупная тема разбивается на отдельные задания. Традиционные материальные результаты обсуждения таковы: составление списка интересных мыслей, выступление одного или двух членов подгрупп с докладами, составление методических разработок или инструкций, составление плана действий.

Экзамен. Обучающиеся обязаны сдать экзамен в соответствии с расписанием и учебным планом. Экзамен – проверочное испытание по учебной дисциплине, конечная форма изучения предмета, а также механизм выявления и оценки результатов учебного процесса. Цель экзамена – проверить сложившуюся у обучающегося систему понятий и отметить степень полученных знаний.

Самостоятельная работа по дисциплине включает следующие виды работ:

– работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы;
– изучение материала, вынесенного на самостоятельную проработку;
– подготовка к семинарским занятиям;
– написание реферата и эссе по заданной проблеме.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

8.1 Перечень информационных технологий.

– Предоставление доступа всем участникам образовательного процесса к корпоративной сети университета и глобальной сети Интернет.
– Предоставление доступа участникам образовательного процесса через сеть Интернет к справочно-поисковым информационным системам.
– Использование специализированного (Офисное ПО, графические, видео- и аудиоредакторы и пр.) программного обеспечения для подготовки тестовых, методических и учебных материалов.
– Использование офисного и мультимедийного программного обеспечения при проведении занятий и для самостоятельной подготовки обучающихся.

8.2 Перечень необходимого программного обеспечения.

– Microsoft Windows , Microsoft Office Professional Plus;
– Acrobat Reader DC; Sumatra PDF ;
– Mozilla FireFox;
– Медиаплеер VLC;
– Архиватор 7– zip;
– Gimp 2.6.16 (растровый графический редактор);
– Inkscape 0.91 (векторный графический редактор).

8.3 Перечень информационных справочных систем:

Научная электронная библиотека (НЭБ) «eLibrary.ru». - URL:http://www.elibrary.ru

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

№	Вид работ	Материально-техническое обеспечение дисциплины и оснащенность
1.	Лекционные занятия	**Аудитории для проведения занятий лекционного типа:** Аудитория 13 оснащена учебной мебелью; Аудитория 14 оснащена учебной мебелью, Аудитория 23 оснащена учебной мебелью, стационарным мультимедийным комплексом в составе: проектор, экран настенный, персональный компьютер с программным обеспечением. Аудитория 24 оснащена учебной мебелью, стационарным мультимедийным комплексом в составе: проектор, экран настенный, персональный компьютер с программным обеспечением; Аудитория 25 оснащена учебной мебелью, стационарным мультимедийным комплексом в составе: проектор, экран настенный, персональный компьютер с программным обеспечением; Аудитория 26 лаборатория для занятий по информатике; Аудитория 27 лаборатория информационных технологий в профессиональной деятельности; Аудитория 28 лаборатория информационно-коммуникационных систем; Аудитория 32 оснащена учебной мебелью; Аудитория 34 оснащена учебной мебелью, стационарным мультимедийным комплексом в составе: проектор, экран настенный, персональный компьютер с программным обеспечением; государственная символика (герб РФ, флаг РФ; флаг Краснодарского края, флаг г. Армавира), Аудитория 35 оснащена учебной мебелью; Аудитория 36 оснащена учебной мебелью.
2.	Практические занятия	**Аудитории для проведения занятий семинарского типа** Аудитория 13 оснащена учебной мебелью; Аудитория 14 оснащена учебной мебелью; Аудитория 23 оснащена учебной мебелью, стационарным мультимедийным комплексом в составе: проектор, экран настенный, персональный компьютер с программным обеспечением. Аудитория 24 оснащена учебной мебелью, стационарным мультимедийным комплексом в составе: проектор, экран настенный, персональный компьютер; Аудитория 25 оснащена учебной мебелью, стационарным мультимедийным комплексом в составе: проектор, экран настенный, персональный компьютер с программным обеспечением; Аудитория 26 лаборатория для занятий по информатике; Аудитория 27 лаборатория информационных технологий в профессиональной деятельности; Аудитория 28 лаборатория информационно-коммуникационных систем; Аудитория 32 оснащена учебной мебелью; Аудитория 34 оснащена учебной мебелью, стационарным мультимедийным комплексом в составе: проектор, экран

		настенный, персональный компьютер, программное обеспечение; государственная символика (герб РФ, флаг РФ; флаг Краснодарского края, флаг г. Армавира), Аудитория 35 оснащена учебной мебелью; Аудитория 36 оснащена учебной мебелью; Аудитория 37 оснащена учебной мебелью, пособия наглядные по иностранному языку: учебные материалы, цветные карты, таблицы.
3.	Групповые (индивидуальные) консультации	**Аудитории для групповых и индивидуальных консультаций:** Аудитория 13 оснащена учебной мебелью; Аудитория 14 оснащена учебной мебелью, Аудитория 23 оснащена учебной мебелью, стационарным мультимедийным комплексом в составе: проектор, экран настенный, персональный компьютер с программным обеспечением; Аудитория 24 оснащена учебной мебелью, стационарным мультимедийным комплексом в составе: проектор, экран настенный, персональный компьютер с программным обеспечением; Аудитория 25 оснащена учебной мебелью, стационарным мультимедийным комплексом в составе: проектор, экран настенный, персональный компьютер с программным обеспечением; Аудитория 26 лаборатория для занятий по информатике; Аудитория 27 лаборатория информационных технологий в профессиональной деятельности; Аудитория 28 лаборатория информационно-коммуникационных систем; Аудитория 32 оснащена учебной мебелью; Аудитория 34 оснащена учебной мебелью, стационарным мультимедийным комплексом в составе: проектор, экран настенный, персональный компьютер с программным обеспечением; государственная символика (герб РФ, флаг РФ; флаг Краснодарского края, флаг г. Армавира), барьер для подсудимого; молоток судьи; табуляторы; портреты выдающихся юристов; наглядные пособия по юриспруденции; Аудитория 35 оснащена учебной мебелью; Аудитория 36 оснащена учебной мебелью; Аудитория 37 оснащена учебной мебелью, материалы, цветные карты, таблицы.
4.	Текущий контроль, промежуточная аттестация	**Аудитории для текущего контроля и промежуточной аттестации:** Аудитория 13 оснащена учебной мебелью; Аудитория 14 оснащена учебной мебелью, Аудитория 23 оснащена учебной мебелью, стационарным мультимедийным комплексом в составе: проектор, экран настенный, персональный компьютер с программным обеспечением; Аудитория 24 оснащена учебной мебелью, стационарным мультимедийным комплексом в составе: проектор, экран

		настенный, персональный компьютер; Аудитория 25 оснащена учебной мебелью, стационарным мультимедийным комплексом в составе: проектор, экран настенный, персональный компьютер с программным обеспечением; Аудитория 26 лаборатория для занятий по информатике; Аудитория 27 лаборатория информационных технологий в профессиональной деятельности; Аудитория 28 лаборатория информационно-коммуникационных систем; Аудитория 32 оснащена учебной мебелью; Аудитория 34 оснащена учебной мебелью, стационарным мультимедийным комплексом в составе: проектор, экран настенный, персональный компьютер с программным обеспечением; государственная символика (герб РФ, флаг РФ; флаг Краснодарского края, флаг г. Армавира); Аудитория 35 оснащена учебной мебелью; Аудитория 36 оснащена учебной мебелью; Аудитория 37 оснащена учебной мебелью; пособия наглядные по иностранному языку: учебные материалы, цветные карты, таблицы.
5.	Самостоятельная работа	**Помещения для самостоятельной работы, с рабочими местами, оснащенными компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации:** Помещение для самостоятельной работы № 18 оснащено учебной мебелью, персональными компьютерами – 4 шт., один из персональных компьютеров, оснащен накладками на клавиатуру со шрифтом Брайля, колонками и наушниками, электронной программой для чтения вслух текстовых файлов «Балаболка» с синтезатором речи с открытым исходным кодом RHVoice. МФУ, программное обеспечение; специализированная мебель: стеллажи библиотечные, шкаф картотечный, библиотечный стол-барьер кафедра для выдачи литературы.