МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ИЖЕВСКАЯ ГОСУДАРСТВЕННАЯ СЕЛЬСКОХОЗЯЙСТВЕННАЯ АКАДЕМИЯ»

УТВЕРЖДАЮ

Проректор по учебной и воспитательной работе

_____ С.Л. Воробьева

"17" 06 2019 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине

Информационная безопасность

Квалификация _____ бакалавр

Направление подготовки 09.03.03 Прикладная информатика

г. Ижевск, 2019

1 ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ С УКАЗАНИЕМ АКАДЕМИЧЕСКИХ ЧАСОВ, ВЫДЕЛЕННЫХ НА КОНТАКТНУЮ РАБОТУ ОБУЧАЮЩИХСЯ С ПРЕПОДАВАТЕЛЕМ (ПО ВИДАМ УЧЕБНЫХ ЗАНЯТИЙ) И НА САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ:

Трудоемкость освоения дисциплины (модуля) составляет _4_ ЗЕТ.

По очной форме обучения:

Отчетность (семестр)		**Всего учебных занятий по дисциплине (модулю)** *(в академических часах)*	144
Экзамен(ы)	7		
Зачет(ы)		*Контактная работа*, в т.ч.:	
Курсовой проект		Лекции	16
Курсовая работа		лабораторные	32
Контрольная(ые) работа(ы)		практические (семинарские)	
Реферат(ы)		*Самостоятельная работа*	51
Эссе		Экзамен(ы)	45
РГР		Зачет(ы)	

По заочной форме обучения:

Отчетность (семестр)		**Всего учебных занятий по дисциплине (модулю)** *(в академических часах)*	144
Экзамен(ы)	9	*Контактная работа*, в т.ч.:	
Зачет(ы)		Лекции	8
Курсовой проект		лабораторные	16
Курсовая работа		практические (семинарские)	
Контрольная(ые) работа(ы)			
Реферат(ы)		*Самостоятельная работа*	75
Эссе		Экзамен(ы)	45
РГР		Зачет(ы)	

2 ЯЗЫК ПРЕПОДАВАНИЯ

Изучение дисциплины осуществляется на русском языке.

3 ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ (МОДУЛЯ)

Целью изучения дисциплины “Информационная безопасность” является формирование у студентов профессиональных компетенций, связанных с использованием теоретических и практических знаний в области обеспечения информационной безопасности при проектировании, внедрении и эксплуатации информационных систем. Содержание курса призвано показать значимость решения проблем обеспечения информационной безопасности экономических информационных систем.

Задачи: Знать теорию безопасного обращения с информацией:

Уметь передавать, хранить и безопасно извлекать информацию;

Научиться защищать информацию от компьютерных вирусов, несанкционированного использования;

Знать правовые основы защиты информации.

4 ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ) СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ (ИНДИКАТОРЫ ДОСТИЖЕНИЯ КОМПЕТЕНЦИЙ)

Таблица 1

Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Код компетенции	Формулировка компетенции	Индикаторы достижения компетенции (связанные с данной дисциплиной)
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	**Знает** основные понятия и составляющие информационной безопасности, виды угроз информационной безопасности**, понятие политики безопасности,** нормативные документы и законодательные акты в области обеспечения информационной безопасности, методы и средства защиты информационных систем**.** **Умеет** объяснить процесс выбора подходящих нормативных и правовых документов. **Умеет применять** нормативно-правовую базу.

5 МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина относится к обязательной части.

6 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ), СТРУКТУРИРОВАННОГО ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

6.1 Распределение видов и часов занятий по семестрам

Таблица 2

Бюджет времени с учетом семестром и видов занятий

Вид учебной работы	Количество часов в семестр по формам обучения		
	очной	очно-заочной	заочной
Семестр	7		8
Аудиторные занятия, в т.ч.:	48		24
- лекции	16		8
- лабораторные работы	32		16
- практические занятия	-		-
- семинары	-		-
Контроль самостоятельной работы	-		-
Самостоятельная работа, в т.ч.:	51		75
- проработка теоретического курса	26		35
- курсовая работа (проект)	-		-
- расчетно-графические работы	-		-
- реферат	-		-
- эссе	-		-
- подготовка к практическим (семинарским) занятиям, выполнение домашнего задания	-		-
- подготовка к выполнению и защите лабораторных работ	32		40
- самотестирование	-		-
- подготовка к зачету (включая его сдачу)	-		-
Самостоятельная работа при подготовке к экзамену, предэкзаменационные консультации и сдача экзамена	45		45
Итого	**144**		**144**
Вид промежуточной аттестации	Экзамен		Экзамен

6.2 Тематический план изучения дисциплины

Таблица 3

Тематический план
с указанием выделенных академических часов на освоение каждого из разделов

№	Наименование разделов, тем	Количество часов по очной форме обучения				Всего часов
		Контактная работа			Самостоятельная работа	
		Лекции	Практические (сем.) занятия	Лабораторные работы		
1	Тема 1. Введение в информационную безопасность.	2			2	4
2	Тема 2. Законодательный уровень обеспечения информационной безопасности.	3		4	6	13
3	Тема 3. Стандарты и спецификации в области информационной безопасности.	3			4	7
4	Тема 4. Сетевая безопасность.	2		8	14	24
5	Тема 5. Вредоносное программное обеспечение и средства защиты от него.				4	4
6	Тема 6. Введение в криптографию.	6		20	21	47
7	Подготовка к экзамену, предэкзаменационные консультации и сдача экзамена				45	45
	Итого часов	**16**		**32**	**96**	**144**

6.3 Теоретический курс

Таблица 4

Основные вопросы, освещаемые на лекциях

Раздел, тема учебной дисциплины, содержание темы
Тема 1. Введение в информационную безопасность.
1.1. Понятие информационной безопасности. Информационная безопасность в условиях функционирования в России глобальных сетей. 1.2. Понятие угрозы. Классификация угроз. 1.3. Аспекты ИБ: доступность, целостность, конфиденциальность. Угрозы доступности. Угрозы целостности. Угрозы конфиденциальности.
Тема 2. Законодательный уровень обеспечения информационной безопасности.
2.1. Назначение и задачи в сфере обеспечения ИБ на уровне государства. Доктрина ИБ РФ. Правовые акты РФ, затрагивающие вопросы ИБ. Ст. 23,24 Конституции РФ. Гражданский кодекс: банковская, коммерческая и служебная тайна. 2.2. Глава 28 УК РФ. Закон «О государственной тайне». Закон «О лицензировании отдельных видов деятельности». Закон «Об электронной цифровой подписи». Закон «О коммерческой тайне». 2.3. Закон «О персональный данных».

Тема 3. Стандарты и спецификации в области информационной безопасности.
3.1. Международные стандарты и спецификации. Стандарт МО США «Критерии оценки доверенных систем» («Оранжевая книга»). Техническая спецификация X.800. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий» («Общие критерии»). Гармонизированные критерии Европейских стран. Интерпретация «Оранжевой книги» для сетевых конфигураций. Британский стандарт BS 7799. 3.2. Российские стандарты и спецификации.
Тема 4. Сетевая безопасность.
4.1. Проблемы безопасности протоколов TCP/IP. Прослушивание сети. Сканирование сети. Генерация пакетов. Сетевые атаки. 4.2. Меры сетевой безопасности. Системы обнаружения атак. Средства анализа защищенности. Экранирование и межсетевые экраны. Общие меры по повышению безопасности сети. 4.3. Протоколы обеспечения безопасности трафика.
Тема 5. Вредоносное программное обеспечение и средства защиты от него.
5.1. Программные закладки: определения и классификация. 5.2. Понятие вируса. Классификация вирусов по различным признакам. 5.3.Защита от вредоносного ПО.
Тема 6. Введение в криптографию.
6.1. Понятие криптографии. Основные определения. Классификации криптоалгоритмов 6.2. Симметричные алгоритмы. 6.3. Асимметричные алгоритмы. 6.4. Хэш-функции. Коды аутентификации сообщений. 6.5. Электронно-цифровая подпись.

6.5 Лабораторный практикум

Таблица 5

Основные темы лабораторного практикума

Номер	Наименование темы лабораторного занятия
1	Разработка программы разграничения полномочий пользователей на основе парольной аутентификации с использованием функций криптографического интерфейса Windows для защиты информации
2	Работа с персональными данными

3	Анализ сетевого трафика
4	Криптографические алгоритмы.

6.7 Самостоятельная работа обучающихся

Таблица 6

Вопросы, изучаемые и прорабатываемые обучающимися самостоятельно

Виды СРС	Номера разделов и тем дисциплины	Сроки выполнения		
		Очная форма	Очно-заочная форма	Заочная форма
Самостоятельная работа в процессе проработки лекционного материала по конспектам и учебной литературе	1-6	1--16 нед. 7 сем.		1--16 нед. 8 сем.
Самостоятельная работа в процессе подготовки к лабораторным занятиям	2,3,4,6	2-16 нед. 7 сем.		2-16 нед. 8 сем.
Самостоятельная работа при подготовке к экзамену	1-6	15-16 нед. 7 сем.		15-16 нед. 8 сем.

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

Оценочные средства представлены в Приложении.

8 ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Основная литература

№ п/п	Наименование	Автор(ы)	Год и место издания	Используется при изучении разделов	Количество экземпляров	
					в библиотеке	на кафедре
1	Кодирование и защита информации : учебное пособие	Акмаров П.Б.	Ижевская ГСХА, 2016	1,2,3,4,5	ЭБС «Руконт» http://rucont.ru/efd/363163	
2	Экономическая информатика. Ч. I. Основные категории и понятия информатики. Задачи экономической информатики на современном этапе. Технические средства информационных систем.	Колганов Е. А.	Уфим. гос. ун-т экономики и сервиса, Финансовый ун-т при Правительстве РФ (Уфим. ф-л), Е. А.	1,2,3	ЭБС «Руконт» http://rucont.ru/efd/314970	

	Персональные компьютеры. Программное обеспечение : учебное пособие		Колганов .— Уфа : УГУЭС, 2014 .		

Дополнительная литература

№ п/п	Наименование	Автор(ы)	Год и место издания	Используется при изучении разделов	Количество экземпляров	
					в библиотеке	на кафедре
1	Основы работы в Excel	Левин Л.А	Красноярск.: КГТИ, 2002	2,3	ЭБС»Руконт»	
3	Закон РФ от 20 февраля 1995 года «Об информации, информатизации и защите информации» № 24-ФЗ		М.: РГ	4,5	ИСС «Консультант-Плюс»	

10 Перечень Интернет-ресурсов

1. Интернет-портал ФГБОУ ВО «Ижевская ГСХА» (http: portal/izhgsha.ru);

2. Сайт http: pravo/gov.ru

11 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

При подготовке к лекции студент может, используя рабочую программу дисциплины, уяснить тему лекции и вопросы, которые будет раскрывать преподаватель при изучении дисциплины. Преподаватель раскрывает наиболее важные, принципиальные вопросы каждой темы, способствующие пониманию логики построения курса, структуры и содержания основных понятий. В конце лекции преподаватель, как правило, формулирует задание для самостоятельной работы студента: изучение определенных разделов учебника, дополнительной литературы, материалов форумов или официальной документации, которые позволят студенту углубить понимание темы и подготовиться выполнению лабораторных работ.

Лабораторные занятия проводятся в соответствии с рабочей программой (раздел 6.5) при последовательном изучении тем дисциплины и представляют собой выполнение обучаемыми набора практических задач предметной области с целью выработки у них навыков их решения (разработки компьютерных программ, с использованием различных графических технологий, а также выполнение задания по работе с различными графическими пакетами). Перед проведением лабораторного занятия по решению задач преподаватель информирует студентов о теме занятия, сообщает о целях и задачах проведения практического занятия, порядке его проведения и критериях оценки результатов работы. Особое внимание при этом студентам следует обратить на особенности работы с теми или иными технологиями и инструментами, необходимыми для решения задач по указанной преподавателем теме занятия.

На лабораторном занятии студентам выдаются (по вариантам) задания на его выполнение. При необходимости преподаватель отвечает на вопросы, помогает разобраться с нюансами инструментов или технологий. После выполнения происходит демонстрация студентом своей разработки и беседа с преподавателем. В случае необходимости преподаватель может давать небольшие задания на доработку, если в процессе собеседования останутся какие-то вопросы или исходное задание будет выполнено не в полном объеме по истечению срока.

Самостоятельная работа является необходимой и обязательной для каждого обучающегося, ее объем по курсу «Информационная безопасность» определяется данной рабочей программой дисциплины. Самостоятельная работа – это изучение без участия преподавателя отдельных тем (вопросов темы), рекомендованных в рабочей программе по данной дисциплине. Главная задача самостоятельной работы – развитие самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня. Самостоятельная работа студентов делится на два вида: аудиторную; внеаудиторную. Видами самостоятельной работы студента в аудиторное время являются: решение задач в рамках лабораторных занятий, участие студента в собеседованиях и т.д. Аудиторная самостоятельная работа студентов организуется и проходит под контролем преподавателя, предполагает выдачу студентам групповых или индивидуальных заданий и самостоятельное выполнение их студентами под методическим и организационным руководством преподавателя. Внеаудиторная работа студента включает: изучение справочной, учебной основной и дополнительной литературы в соответствии с рекомендациями в рабочей программе по данной дисциплине; выполнение курсовой работы.

12 ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ), ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

№ п\п	Наименование специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения (подлежит ежегодному обновлению)
1	Учебные аудитории для проведения занятий лекционного типа, текущего контроля и промежуточной аттестации	Microsoft Windows XP и выше; Архиватор 7-Zip; Антивирус DR-web; Adobe Reader X; Microsoft Office.
2	Специализированные лаборатории для проведения лабораторных занятий групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Microsoft Windows XP и выше; Архиватор 7-Zip; Антивирус DR-web; Adobe Reader X; Microsoft Office; Microsoft Access,
3	Помещения для самостоятельной работы (читальный зал научной библиотеки)	Microsoft Windows XP и выше; Архиватор 7-Zip; Антивирус DR-web; Adobe Reader X; Microsoft Office.

13 ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

№ п\п	Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
1	Учебные аудитории для проведения занятий лекционного типа, текущего контроля и промежуточной аттестации	Учебная мебель: столы, стулья для обучающихся; стол, стул для преподавателя, доска магнитно-маркерная. Аудитория, оснащенная комплексом технических средств обучения (проектор, экран, компьютер)
2	Специализированные лаборатории для проведения лабораторных занятий групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Учебная мебель: столы, стулья для обучающихся; стол, стул для преподавателя. Компьютеры, объединенные в ЛВС, с выходом в Интернет
3	Помещения для самостоятельной работы (читальный зал научной библиотеки)	Рабочие места, оборудованные ПЭВМ с выходом в Интернет (Wi-Fi)

Фонд оценочных средств (оценочных материалов) для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Оценочные материалы, используемые для проведения текущего контроля и промежуточной аттестации представлены в таблице П1.

Таблица П1

№ п/п	Код и наименование формируемой компетенции	Наименование оценочного средства*
1	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	Тест, собеседование по лабораторным работам, экзамен

** Тест, собеседование по практических (семинарским) занятиям, собеседование по лабораторным работам, курсовое проектирование, реферат, РГР и т.п., зачет, зачет с оценкой, экзамен*

П.2.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

При изучении дисциплин студент осваивает компетенции ОПК-3, на этапе указанном в п.3 характеристики образовательной программы.

П.2.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание их шкал оценивания

Собеседование по лабораторным работам

Собеседование по выполнению лабораторных работ осуществляется с целью проверки уровня знаний, умений, владений, понимания студентом основных методов и методик работы с графическими технологиями и инструментами при решении конкретных практических задач, умения применять на практике полученных знаний. Каждое лабораторное занятие студент выполняет объемную задачу по конкретной теме с возможностью внесения доработок и изменений. Общее число лабораторных занятий – 4. Шкала оценивания имеет вид (таблица П3)

Таблица П2

Шкала и критерии оценивания решения задач на лабораторных занятиях

Оценка	Критерии
Отлично	Студент демонстрирует знания теоретического и практического материала по теме лабораторной работы, дает правильный алгоритм решения, в конце занятия студент выдает законченную и полностью функционирующую разработку.
Хорошо	Студент демонстрирует знания теоретического и практического материала по теме практической работы, допуская незначительные неточности при решении задач, в конце занятия студент выдает неполностью функционирующую разработку
Удовлетворительно	Студент затрудняется с правильной оценкой предложенной задачи, выбор алгоритма решения задачи возможен при наводящих вопросах преподавателя, в конце занятия студент выдает незаконченную, но частично функционирующую разработку.
Неудовлетворительно	Студент в конце занятия не выдает хоть сколько-нибудь функ-

	ционирующей разработки, некорректно отвечает на дополнительные вопросы.

Тест

В ходе тестирования студенту дается 10 вопросов. Шкала оценивания имеет вид (таблица П2)

Таблица П2

Шкала и критерии оценивания выполнения теста

Оценка	Критерии
Отлично	Студент правильно ответил не менее чем на 9 из 10 вопросов
Хорошо	Студент правильно ответил не менее чем на 7 из 10 вопросов
Удовлетворительно	Студент правильно ответил не менее чем на 5 из 10 вопросов
Неудовлетворительно	Студент правильно ответил менее чем на 5 из 10 вопросов

Экзамен

Экзамен имеет своей целью проверить и оценить уровень полученных студентами знаний и умение применять их к решению практических задач, овладение практическими навыками и умениями в объеме требований учебной программы, а также качество и объем индивидуальной работы студентов.

К экзамену допускаются студенты, выполнившие все лабораторные работы в соответствии с требованиями учебной программы.

Экзамен принимает преподаватель, ведущий лекционные занятия по данной дисциплине. Экзамен проводится в объеме рабочей программы по билетам. При проведении экзамена в каждый билет включаются три. Билетов должно быть на 20% больше числа студентов в учебной группе. Предварительное ознакомление студентов с билетами не разрешается. Кроме указанных в билете вопросов преподаватель имеет право задавать дополнительные вопросы с целью уточнения объема знаний студентов и оценки качества усвоения теоретического материала и практических навыков и умений.

Шкала оценивания имеет вид (таблица П7)

Таблица П3

Шкала и критерии оценивания экзамена

Оценка	Критерии
Отлично	Выставляется обучающемуся, если студент показал глубокие знания теоретического материала по поставленному вопросу, грамотно логично и стройно его излагает, а также выполнил в полном объеме практическое задание и способен обосновать свои решения
Хорошо	Выставляется обучающемуся, если студент твердо знает теоретический материал, грамотно его излагает, не допускает существенных неточностей в ответе на вопрос, выполнил практическое задание не в полном объеме (не менее ¾) либо в полном объеме, но с несущественными погрешностями и ошибками
Удовлетворительно	выставляется обучающемуся, если студент показывает знания только основных положений по поставленному вопросу, требует в отдельных случаях наводящих вопросов для принятия правильного решения, допускает отдельные неточности; выполнил практическое задание не в полном объеме (не менее ½) либо в полном объеме, но с существенными погрешностями и ошибками
Неудовлетворительно	выставляется обучающемуся, если студент допускает грубые ошибки в ответе на поставленный вопрос, не справился с выполнением практического задания

П.2.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Перечень контрольных вопросов к экзамену

Тема 1. Введение в информационную безопасность.

1. Понятие информационной безопасности. Компьютерная безопасность.
2. Доктрина ИБ РФ.
3. Понятие угрозы, атаки, источника угроз, окна опасности. Классификация угроз.
4. Угрозы доступности.
5. Угрозы целостности.
6. Угрозы конфиденциальности.

Тема 2. Законодательный уровень обеспечения информационной безопасности.

1. Законодательный уровень обеспечения ИБ. Конституция РФ.
2. УК РФ в области защиты информации.
3. Закон «О государственной тайне» и ответственность за его нарушение.
4. Закон «О коммерческой тайне» и меры ответственности за его нарушение.
5. Закон «О персональных данных».
6. Закон «ОБ информации, информационных технологиях и о защите информации».
7. Закон «О лицензировании отдельных видов деятельности». Основные лицензирующие органы и их функции.
8. Нарушение авторских и смежных прав в Гражданском кодексе РФ.
9. Кодекс об административных нарушениях РФ в области защиты информации.

Тема 3. Стандарты и спецификации в области информационной безопасности.

1. Стандарт МО США «Критерии оценки доверенных систем» («Оранжевая книга»). Понятие доверенной системы. Критерии степени доверия.
2. Стандарт МО США «Критерии оценки доверенных систем» («Оранжевая книга»). Понятие доверенной вычислительной базы. Монитор обращений.
3. Механизмы и классы безопасности «Оранжевой книги».
4. Техническая спецификация X.800. Сетевые средства безопасности. Сетевые механизмы безопасности. Администрирование средств безопасности.
5. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий» («Общие критерии»). Требования безопасности. Угрозы и уязвимые места. Профили защиты.
6. «Общие критерии». Функциональный пакет. Функциональные требования. Требования доверия безопасности.
7. Руководящие документы Гостехкомиссии РФ. Классификация МЭ. ГОСТы.

Тема 4. Сетевая безопасность.

1. Прослушивание и сканирование сети. Генерация пакетов.
2. Перехват данных.
3. Имперсонация. Несанкционированный обмен данными. Принуждение к ускоренной передаче данных.
4. Отказ в обслуживании. Классификация и типы атак.
5. Системы обнаружения атак. Классификация.
6. Средства анализа защищенности: сканирование, зондирование.
7. Экранирование и межсетевые экраны. Основные понятия. Принципы работы межсетевых экранов.
8. Классификация межсетевых экранов. Понятие демилитаризованной зоны.
9. Пакетные фильтры. Сервера уровня соединения. Сервера прикладного уровня.
10. Протокол SSL.
11. Протокол SSH.

12. Протокол S-HTTP.
13. Протокол SOCKS.
14. Протокол безопасности IPSec как набор стандартов для защиты данных и аутентификации на уровне IP. Туннельный и транспортный режим.
15. VPN и протоколы туннелирования.

Тема 5. Вредоносное программное обеспечение и средства защиты от него.

1. Программные закладки: определения и классификация.
2. Модели воздействия программных закладок на компьютеры. Способы воздействия на ЭЦП.
3. Защита от программных закладок. Понятие изолированного компьютера.
4. Троянские программы. Утилиты скрытого администрирования. Клавиатурные шпионы и их типы. Парольные взломщики.
5. Понятие вируса. Классификация вирусов по различным признакам.
6. Полиморфик-вирусы. Загрузочные вирусы. Макро-вирусы. Сетевые вирусы. Файловые вирусы.
7. Антивирусное ПО. Классификация.

Тема 6. Введение в криптографию.

1. Понятие криптографии. Основные определения. Классификация криптоалгоритмов по принципу действия.
2. Симметричные и асимметричные алгоритмы. Классификация криптоалгоритмов по характеру воздействия на шифруемую информацию. Классификация по размеру обрабатываемых блоков: блочные и поточные алгоритмы.
3. Сеть Фейстеля.
4. Симметричные криптоалгоритмы, их параметры.
5. Алгоритм ГОСТ 28147. Схема и режимы работы.
6. Асимметричные алгоритмы. Основные требования, принципы действия, характеристики.

Примерный перечень вопросов теста

Защита информации - это
- комплекс мероприятий, направленных на обеспечение информационной безопасности.
- комплекс мероприятий, направленных на обеспечение информационной целостности.
- защита данных от неправомерного доступа.

Информационная безопасность - защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ### ущерб субъектам информационных отношений.
- неприемлемый
- недопустимый

Возможность за приемлемое время получить требуемую информационную услугу - это
- Оперативность
- Доступность
- Открытость
- Целостность

Актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения - это
- Конфиденциальность
- Безопасность

- Целостность
- Доступность

Защита от несанкционированного доступа к информации - это
- Конфиденциальность
- Безопасность
- Целостность
- Закрытость

Динамическая целостность - это
- неизменность информационных объектов
- возможность за приемлемое время получить требуемую информационную услугу
- корректность выполнения транзакций
- защита от несанкционированного доступа к информации

Угроза - это
- Атака
- потенциальная возможность определенным образом нарушить информационную безопасность
- Нестабильность
- невозможность за приемлемое время получить требуемую информационную услугу
- Сканирование

Атака - это
- Попытка взлома системы
- Попытка использования уязвимостей
- Взлом системы
- Попытка реализации угрозы

Окно опасности - это
- Промежуток времени от момента, когда появляется слабое место до момента, когда оно ликвидируется.
- Промежуток времени от момента, когда начинается реализации атаки, и до момента, когда атака заканчивается.
- Незащищённые порты системы.
- Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется.
- Промежуток времени от момента, когда планируется атака, до момента, когда атака заканчивается.

Угрозы можно классифицировать по нескольким критериям:
- по аспекту информационной безопасности
- по доступности
- по компонентам информационных систем, на которые угрозы нацелены
- по способу осуществления
- случайные/преднамеренные действия
- по расположению источника угроз
- нет правильных ответов

Статья 272 УК РФ предусматривает ответственность за:
- произвольный доступ к компьютерной информации
- неправомерный доступ к компьютерной информации
- распространение вредоносных программ для ЭВМ

- нарушение правил эксплуатации ЭВМ

С целью нарушения статической целостности злоумышленник может:
- ввести неверные данные
- изменить данные
- нарушить атомарность транзакций
- украсть данные

Угрозами динамической целостности является:
- нарушение атомарности транзакций
- переупорядочение
- кража
- ввод неверных данных
- нет правильных ответов

Процедурный уровень ИБ.Основной принцип физической защиты, соблюдение которого следует постоянно контролировать, формулируется как
- достоверность защиты в пространстве и времени.
- защита физической среды передачи данных.
- непрерывность защиты в пространстве и времени.

Процедурный уровень ИБ. Принцип разделения обязанностей предписывает так распределять роли и ответственность, чтобы
- один человек не мог нарушить критически важный для организации процесс.
- каждый человек отвечал за необходимую область.

Программно-технический уровень ИБ. Какие сервисы относятся к основным.
- управление доступом
- шифрование
- экранирование
- идентификация и аутентификация
- анализ защищенности
- перечисленные сервисы не относятся к основным

Идентификация позволяет субъекту:
- назвать себя (сообщить свое имя).
- убедиться, что субъект действительно тот, за кого он себя выдает.

Аутентификации позволяет:
- убедиться, что субъект действительно тот, за кого он себя выдает.
- назвать себя (сообщить свое имя).

Меры позволяющие значительно повысить надежность парольной защиты:
- наложение технических ограничений
- ограничение доступа к файлам других пользователей
- управление сроком действия паролей, их периодическая смена
- ограничение доступа к файлу паролей
- блокирование пользователей, при долговременной неактивности
- ограничение числа неудачных попыток входа в систему

Sniffing - это
- прослушивание
- создание IP-датаграмм или кадров уровня доступа к сети, направленных якобы от другого узла

– подмена маршрутизатора

Spoofing - это
– прослушивание
– создание IP-датаграмм или кадров уровня доступа к сети, направленных якобы от другого узла
– подмена маршрутизатора

П.2.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Оценка знаний, умений, навыков может быть выражена в параметрах:

- «очень высокая», «высокая», соответствующая академической оценке «отлично»;
- «достаточно высокая», «выше средней», соответствующая академической оценке «хорошо»;
- «средняя», «ниже средней», «низкая», соответствующая академической оценке «удовлетворительно»;
- «очень низкая», «примитивная», соответствующая академической оценке «неудовлетворительно».

Критерии оценивания:

- полнота знаний теоретического контролируемого материала;
- полнота знаний практического контролируемого материала, демонстрация умений и навыков решения типовых задач, выполнения типовых заданий/упражнений/казусов;
- умение извлекать и использовать основную (важную) информацию из заданных теоретических, научных, справочных, энциклопедических источников;
- умение собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников;
- умение собирать, систематизировать, анализировать и грамотно использовать практический материал для иллюстраций теоретических положений;
- умение самостоятельно решать проблему/задачу на основе изученных методов, приемов, технологий;
- умение ясно, четко, логично и грамотно излагать собственные размышления, делать умозаключения и выводы;
- умение соблюдать заданную форму изложения (доклад, эссе, другое);
- умение пользоваться ресурсами глобальной сети (интернет);
- умение пользоваться нормативными документами;
- умение создавать и применять документы, связанные с профессиональной деятельностью;
- умение определять, формулировать проблему и находить пути ее решения;
- умение анализировать современное состояние отрасли, науки и техники;
- умение самостоятельно принимать решения на основе проведенных исследований;
- умение и готовность к использованию основных (изученных) прикладных программных средств;
- умение создавать содержательную презентацию выполненной работы.

Критерии оценки компетенций:

- знание возможностей различных графических технологий;
- знание способов работы с той или иной графической технологией;
- знание возможностей основных графический инструментов;
- умение использовать различные графически технологии для разработки программных интерфейсов;

- умение осуществлять подбор графических инструментов, необходимых для оформления презентаций и научно-технических отчетов;
- умение проводить исследование возможностей технологий;
- владение навыками работы с различными графическими технологиями;
- владение навыками работы с различными графическими инструментами;
- владение навыками оформления отчета по результатам этого исследования;

Средства оценивания для контроля

Собеседование – средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п. Для повышения объективности оценки собеседование может проводиться группой преподавателей/экспертов. Критерии оценки результатов собеседования зависят от того, каковы цели поставлены перед ним и, соответственно, бывают разных видов:

Тест - набор вопросов, как с вариантами ответа так и без них,

Лабораторная работа - работа обучающегося с целью формирования у обучаемых умений и навыков профессиональной практической работы. Результаты работы оформляются в виде программы и содержат решение профессиональной задачи и составление профессионального суждения о полученных результатах работы в виде выводов.

Экзамен – процедура, проводимая по установленным правилам для оценки чьих-либо знаний, умений, компетенций по какому-либо учебному предмету, модулю и т.д. Процедура проведения экзамена может быть организована по-разному.