Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Ашмарина Светлана Игоревна
Должность: Ректор ФГБОУ ВО «Самарский государственный экономический университет»
Дата подписания: 29.01.2021 12:37:57
Уникальный программный ключ:
59650034d6e3a6baac49b7bd0f8e79fea1433ff3e82f1fc7e9279a031181baba

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Самарский государственный экономический университет»

Институт права

Кафедра Теории права и философии

УТВЕРЖДЕНО
Ученым советом Университета
(протокол № 10 от 29 апреля 2020 г.)

РАБОЧАЯ ПРОГРАММА

Наименование дисциплины Б1.В.04 Информационная безопасность

Основная профессиональная образовательная программа 38.05.01 ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ
программа специализация N 1
"Экономико-правовое обеспечение экономической безопасности"

Методический отдел УМУ
«16» 04 2020 г.
_____/_____/

Научная библиотека СГЭУ
«16» 04 2020 г.
_____/_____/

Рассмотрено к утверждению
на заседании кафедры Теории права и философии
(протокол № 8 от 05.03.2020г.___)
Зав. кафедрой_____/_А.В. Гурьянова__/

Квалификация (степень) выпускника экономист

Самара 2020

Содержание (рабочая программа)

Стр.

Целью изучения дисциплины является формирование результатов обучения, обеспечивающих достижение планируемых результатов освоения образовательной программы.

1. Место дисциплины в структуре ОП

Дисциплина Информационная безопасность входит в вариативную часть блока Б1.Дисциплины (модули)

Предшествующие дисциплины по связям компетенций: Информатика

Последующие дисциплины по связям компетенций: Информационные системы в экономике, Лабораторный практикум по налоговым расчетам в системе экономической безопасности, Электронные носители отчетности, Государственный аудит, Экономический анализ, Бухгалтерская (финансовая) отчетность, Комплексный экономический анализ финансово-хозяйственной деятельности, Контроль и ревизия, Деньги, кредит, банки , Анализ финансовой отчетности, Лабораторный практикум по бухгалтерскому учету в системе 1С, Бюджетный учет и отчетность, Международные стандарты финансовой отчетности, Оценка бизнеса

2. Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов обучения по программе

Изучение дисциплины Информационная безопасность в образовательной программе направлено на формирование у обучающихся следующих компетенций:

Общекультурные компетенции (ОК):

ОК-12 - способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
ОК-12	Знать	Уметь	Владеть (иметь навыки)
	ОК12з1: основные методы и средства поиска, систематизации, обработки, передачи и защиты информации	ОК12у1: классифицировать и определять объем информации, представленной в различном виде; решать стандартные задачи профессиональной деятельности на основе информационной культуры	ОК12в1: стандартными средствами базовых информационных процессов и технологий; основными методами, способами и средствами получения, хранения, поиска, систематизации, обработки, передачи и защиты информации
	ОК12з2: современные программные продукты, необходимые для решения профессиональных задач	ОК12у2: работать с различными информационными ресурсами и технологиями, использовать методы и средства обеспечения информационной безопасности с целью предотвращения несанкционированного доступа, злоумышленной модификации или утраты	ОК12в2: навыками работы с информационно-поисковыми и информационно-справочными системами и базами данных, используемыми в профессиональной деятельности; культурой применения информационно-коммуникационных технологий с учетом

		информации, составляющей государственную тайну, и иной служебной информации	основных требований информационной безопасности

Профессиональные компетенции (ПК):

ПК-29 - способностью выбирать инструментальные средства для обработки финансовой, бухгалтерской и иной экономической информации и обосновывать свой выбор

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
ПК-29	Знать	Уметь	Владеть (иметь навыки)
	ПК29з1: роль и место информационных систем в экономике; классификацию ИС по уровням управления, видам ресурсов, процессов, протекающих в экономических системах; состав инструментальных средств для обработки бухгалтерской и финансовой информации	ПК29у1: анализировать состав, функции и возможности справочных и информационно-поисковых систем; выбирать инструментальные средства для обработки разного вида финансовой, бухгалтерской и иной экономической информации	ПК29в1: навыками формирования бухгалтерских документов при помощи инструментальных средств; обоснованного выбора и использования инструментальных средств обработки финансовой и иной экономической информации
	ПК29з2: методы анализа бухгалтерской (финансовой) отчетности; состав и функциональные возможности инструментальных средств и информационных технологий обеспечения экономической безопасности	ПК29у2: выявлять угрозы информационной безопасности на основе инструментальной обработки финансовой, бухгалтерской и иной экономической информации и использования специализированных программных продуктов	ПК29в2: навыками анализа бухгалтерской (финансовой) отчетности, использования специализированных программных продуктов и инструментальных средств для решения профессиональных задач обеспечения экономической безопасности

3. Объем и виды учебной работы

Учебным планом предусматриваются следующие виды учебной работы по дисциплине:

Очная форма обучения

Виды учебной работы	Всего час/ з.е.
	Сем 3
Контактная работа, в том числе:	37.15/1.03
Занятия лекционного типа	18/0.5
Занятия семинарского типа	18/0.5
Индивидуальная контактная работа (ИКР)	0.15/0
Групповая контактная работа (ГКР)	1/0.03
Самостоятельная работа, в том числе:	25.85/0.72
Промежуточная аттестация	9/0.25
Вид промежуточной аттестации: Зачет	Зач
Общая трудоемкость (объем части образовательной	

программы): Часы	72
Зачетные единицы	2

4. Содержание дисциплины

4.1. Разделы, темы дисциплины и виды занятий:

Тематический план дисциплины Информационная безопасность представлен в таблице.

Разделы, темы дисциплины и виды занятий
Очная форма обучения

№ п/п	Наименование темы (раздела) дисциплины	Контактная работа				Самостоятельная работа	Планируемые результаты обучения в соотношении с результатами обучения по образовательной программе
		Лекции	Занятия семинарского типа: Практич. занятия	ИКР	ГКР		
1.	Информация как объект защиты	2	4			1,85	ОК12з1, ОК12з2, ОК12у1, ОК12у2, ОК12в1, ОК12в2, ПК29з1, ПК29з2, ПК29у1, ПК29у2, ПК29в1, ПК29в2
2.	Информационная безопасность	4	2			2	ОК12з1, ОК12з2, ОК12у1, ОК12у2, ОК12в1, ОК12в2, ПК29з1, ПК29з2, ПК29у1, ПК29у2, ПК29в1, ПК29в2
3.	Критерии оценки безопасности компьютерных систем	2	2			2	ОК12з1, ОК12з2, ОК12у1, ОК12у2, ОК12в1, ОК12в2, ПК29з1, ПК29з2, ПК29у1, ПК29у2, ПК29в1, ПК29в2
4.	Криптографические средства защиты информации	2	2			4	ОК12з1, ОК12з2, ОК12у1, ОК12у2, ОК12в1, ОК12в2, ПК29з1, ПК29з2, ПК29у1, ПК29у2, ПК29в1, ПК29в2
5.	Электронная цифровая подпись	2	2			4	ОК12з1, ОК12з2, ОК12у1, ОК12у2, ОК12в1, ОК12в2, ПК29з1, ПК29з2, ПК29у1, ПК29у2, ПК29в1, ПК29в2
6.	Защита от копирования	2	2			4	ОК12з1, ОК12з2, ОК12у1, ОК12у2, ОК12в1, ОК12в2, ПК29з1, ПК29з2, ПК29у1, ПК29у2, ПК29в1, ПК29в2
7.	Программы с потенциально опасными последствиями	2	2			4	ОК12з1, ОК12з2, ОК12у1, ОК12у2,

							ОК12в1, ОК12в2, ПК29з1, ПК29з2, ПК29у1, ПК29у2, ПК29в1, ПК29в2
8.	Защита в интернет	2	2			4	ОК12з1, ОК12з2, ОК12у1, ОК12у2, ОК12в1, ОК12в2, ПК29з1, ПК29з2, ПК29у1, ПК29у2, ПК29в1, ПК29в2
	Контроль	9					
	Итого	**18**	**18**	**0.15**	**1**	**25.85**	

4.2 Содержание разделов и тем

4.2.1 Контактная работа

Тематика занятий лекционного типа

№п/п	Наименование темы (раздела) дисциплины	Вид занятия лекционного типа*	Тематика занятия лекционного типа
1.	Информация как объект защиты	лекция	Введение в защиту информации и информационную безопасность
2.	Информационная безопасность	лекция	Информационная безопасность. Основные угрозы информационной безопасности. Обеспечение информационной безопасности. Аппаратно-программные средства защиты информации
3.	Критерии оценки безопасности компьютерных систем	лекция	Критерии оценки безопасности компьютерных систем. Оранжевая книга. Основные элементы политики безопасности. Классы безопасности.
4.	Криптографические средства защиты информации	лекция	Простые криптосистемы. Шифрование методом замены (подстановки). Шифрование методом перестановки. Шифрование методом гаммирования. Шифрование с помощью аналитических преобразований. Комбинированные методы шифрования. Организационные проблемы криптозащиты.
5.	Электронная цифровая подпись	лекция	Проблема аутентификации данных и электронная цифровая подпись. Однонаправленные хэш-функции. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов. Алгоритм безопасного хэширования SHA. Отечественный стандарт хэш-функции. Алгоритмы электронной цифровой подписи. Алгоритм цифровой подписи Эль Гамаля (EGSA). Алгоритм цифровой подписи DSA. Отечественный стандарт цифровой подписи.

6.	Защита от копирования	лекция	Защита от копирования. Защита CD от копирования. Защиты от несанкционированного доступа. Идентификация и аутентификация пользователя. Протоколы идентификации с нулевой передачей знаний.
7.	Программы с потенциально опасными последствиями	лекция	Программы с потенциально опасными последствиями. Вирус. Люк. Троянский конь. Логическая бомба. Программные закладки. Атака салями.
8.	Защита в интернет	лекция	Межсетевые экраны. Компьютерные атаки и технологии их обнаружения. Безопасность электронной коммерции. Безопасность электронных платежных систем. Идеальная служба информационной безопасности.

*лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях, обучающимся

Тематика занятий семинарского типа

№п/п	Наименование темы (раздела) дисциплины	Вид занятия семинарского типа**	Тематика занятия семинарского типа
1.	Информация как объект защиты	практическое занятие	Средства защиты компьютера от вирусов
2.	Информационная безопасность	практическое занятие	Построение кода постоянной длины
3.	Критерии оценки безопасности компьютерных систем	практическое занятие	Построение кода переменной длины
4.	Криптографические средства защиты информации	практическое занятие	Методы защиты информации. Шифр простой перестановки
5.	Электронная цифровая подпись	практическое занятие	Методы защиты информации. Шифр Цезаря
6.	Защита от копирования	практическое занятие	Модифицированный шифр Цезаря со сдвигом по кодовому слову

7.	Программы с потенциально опасными последствиями	практическое занятие	Архивация информации
8.	Защита в интернет	практическое занятие	Сравнение методов сжатия данных

** семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия

Иная контактная работа

При проведении учебных занятий СГЭУ обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая при необходимости проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплин (модулей) в форме курсов, составленных на основе результатов научных исследований, проводимых организацией, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

Формы и методы проведения иной контактной работы приведены в Методических указаниях по основной профессиональной образовательной программе.

4.2.2 Самостоятельная работа

№п/п	Наименование темы (раздела) дисциплины	Вид самостоятельной работы ***
1.	Информация как объект защиты	- тестирование
2.	Информационная безопасность	- тестирование
3.	Критерии оценки безопасности компьютерных систем	- тестирование
4.	Криптографические средства защиты информации	- тестирование
5.	Электронная цифровая подпись	- тестирование
6.	Защита от копирования	- тестирование
7.	Программы с потенциально опасными последствиями	- тестирование
8.	Защита в интернет	- тестирование

*** самостоятельная работа в семестре, написание курсовых работ, докладов, выполнение контрольных работ

5. Материально-техническое и учебно-методическое обеспечение дисциплины

5.1 Литература:

Основная литература

Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2019. — 325 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/432966

Дополнительная литература

Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с. — (Университеты России). — ISBN 978-5-534-00258-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/434171

Литература для самостоятельного изучения

1. Правовая информатика: учебник и практикум для прикладного бакалавриата / С. Г. Чубукова, Т. М. Беляева, А. Т. Кудинов, Н. В. Пальянова; под редакцией С. Г. Чубуковой. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2019. — 314 с. — (Бакалавр и специалист). — ISBN 978-5-534-03900-9. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/431903 (дата обращения: 16.07.2019). https://biblio-online.ru/book/pravovaya-informatika-431903

Ефанова, Н. Н. Поиск правовой информации: стратегия и тактика / Н. Н. Ефанова. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2019. — 234 с. — (Консультации юриста). — ISBN 978-5-534-04427-0. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/431828 (дата обращения: 16.07.2019). https://biblio-online.ru/book/poisk-pravovoy-informacii-strategiya-i-taktika-431828

5.2. Перечень лицензионного программного обеспечения

1. Microsoft Windows 10 Education / Microsoft Windows 7 / Windows Vista Business
2. Office 365 ProPlus, Microsoft Office 2019, Microsoft Office 2016 Professional Plus (Word, Excel, Access, PowerPoint, Outlook, OneNote, Publisher) / Microsoft Office 2007 (Word, Excel, Access, PowerPoint)
3. Project-Expert 7

5.3 Современные профессиональные базы данных, к которым обеспечивается доступ обучающихся

1. Профессиональная база данных «Информационные системы Министерства экономического развития Российской Федерации в сети Интернет» (Портал «Официальная Россия» - http://www.gov.ru/)
2. Государственная система правовой информации «Официальный интернет-портал правовой информации» (http://pravo.gov.ru/)

5.4. Информационно-справочные системы, к которым обеспечивается доступ обучающихся

1. Справочно-правовая система «Консультант Плюс»
2. Справочно-правовая система «ГАРАНТ-Максимум»

5.5. Специальные помещения

Учебные аудитории для проведения занятий лекционного типа	Комплекты ученической мебели Мульмедийный проектор Доска Экран
Учебные аудитории для проведения практических занятий (занятий семинарского типа)	Комплекты ученической мебели Мульмедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Учебные аудитории для групповых и индивидуальных консультаций	Комплекты ученической мебели Мульмедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС

	СГЭУ
Учебные аудитории для текущего контроля и промежуточной аттестации	Комплекты ученической мебели Мульмедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Помещения для самостоятельной работы	Комплекты ученической мебели Мульмедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Помещения для хранения и профилактического обслуживания оборудования	Комплекты специализированной мебели для хранения оборудования
Кабинет информатики (компьютерный класс)	Комплекты ученической мебели Мульмедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ Лабораторное оборудование

Для проведения занятий лекционного типа используются демонстрационное оборудование и учебно-наглядные пособия в виде презентационных материалов, обеспечивающих тематические иллюстрации.

6. Фонд оценочных средств по дисциплине Информационная безопасность:

6.1. Контрольные мероприятия по дисциплине

Вид контроля	**Форма контроля**	**Отметить нужное знаком « + »**
Текущий контроль	Оценка докладов	-
	Устный/письменный опрос	-
	Тестирование	+
	Практические задачи	+
	Оценка контрольных работ (для заочной формы обучения)	-
Промежуточный контроль	Зачет	+

Порядок проведения мероприятий текущего и промежуточного контроля определяется Методическими указаниями по основной профессиональной образовательной программе высшего образования, утвержденными Ученым советом ФГБОУ ВО СГЭУ №10 от 29.04.2020г.

6.2. Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов обучения по программе

Общекультурные компетенции (ОК):

ОК-12 - способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска,

систематизации, обработки и передачи информации

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
	Знать	Уметь	Владеть (иметь навыки)
Пороговый	ОК12з1: основные методы и средства поиска, систематизации, обработки, передачи и защиты информации	ОК12у1: классифицировать и определять объем информации, представленной в различном виде; решать стандартные задачи профессиональной деятельности на основе информационной культуры	ОК12в1: стандартными средствами базовых информационных процессов и технологий; основными методами, способами и средствами получения, хранения, поиска, систематизации, обработки, передачи и защиты информации
Повышенный	ОК12з2: современные программные продукты, необходимые для решения профессиональных задач	ОК12у2: работать с различными информационными ресурсами и технологиями, использовать методы и средства обеспечения информационной безопасности с целью предотвращения несанкционированного доступа, злоумышленной модификации или утраты информации, составляющей государственную тайну, и иной служебной информации	ОК12в2: навыками работы с информационно -поисковыми и информационно-справочными системами и базами данных, используемыми в профессиональной деятельности; культурой применения информационно-коммуникационных технологий с учетом основных требований информационной безопасности

Профессиональные компетенции (ПК):

ПК-29 - способностью выбирать инструментальные средства для обработки финансовой, бухгалтерской и иной экономической информации и обосновывать свой выбор

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
	Знать	Уметь	Владеть (иметь навыки)
Пороговый	ПК29з1: роль и место информационных систем в экономике; классификацию ИС по уровням управления, видам ресурсов, процессов, протекающих в экономических системах; состав инструментальных средств для обработки	ПК29у1: анализировать состав, функции и возможности справочных и информационно-поисковых систем; выбирать инструментальные средства для обработки разного вида финансовой, бухгалтерской и иной	ПК29в1: навыками формирования бухгалтерских документов при помощи инструментальных средств; обоснованного выбора и использования инструментальных средств обработки финансовой и иной экономической информации

	бухгалтерской и финансовой информации	экономической информации	
Повышенный	ПК29з2: методы анализа бухгалтерской (финансовой) отчетности; состав и функциональные возможности инструментальных средств и информационных технологий обеспечения экономической безопасности	ПК29у2: выявлять угрозы информационной безопасности на основе инструментальной обработки финансовой, бухгалтерской и иной экономической информации и использования специализированных программных продуктов	ПК29в2: навыками анализа бухгалтерской (финансовой) отчетности, использования специализированных программных продуктов и инструментальных средств для решения профессиональных задач обеспечения экономической безопасности

6.3. Паспорт оценочных материалов

№ п/п	Наименование темы (раздела) дисциплины	Контролируемые планируемые результаты обучения в соотношении с результатами обучения по программе	Вид контроля/используемые оценочные средства	
			Текущий	Промежуточный
1.	Информация как объект защиты	ОК12з1, ОК12з2, ОК12у1, ОК12у2, ОК12в1, ОК12в2,	Тестирование Практические задачи	Зачет
2.	Информационная безопасность	ОК12з1, ОК12з2, ОК12у1, ОК12у2, ОК12в1, ОК12в2,	Тестирование Практические задачи	Зачет
3.	Критерии оценки безопасности компьютерных систем	ПК29з1, ПК29з2, ПК29у1, ПК29у2, ПК29в1, ПК29в2	Тестирование Практические задачи	Зачет
4.	Криптографические средства защиты информации	ПК29з1, ПК29з2, ПК29у1, ПК29у2, ПК29в1, ПК29в2	Тестирование Практические задачи	Зачет
5.	Электронная цифровая подпись	ОК12з1, ОК12з2, ОК12у1, ОК12у2, ОК12в1, ОК12в2,	Тестирование Практические задачи	Зачет
6.	Защита от копирования	ПК29з1, ПК29з2, ПК29у1, ПК29у2, ПК29в1, ПК29в2	Тестирование Практические задачи	Зачет
7.	Программы с потенциально опасными последствиями	ОК12з1, ОК12з2, ОК12у1, ОК12у2, ОК12в1, ОК12в2,	Тестирование Практические задачи	Зачет
8.	Защита в интернет	ПК29з1, ПК29з2, ПК29у1, ПК29у2, ПК29в1, ПК29в2	Тестирование Практические задачи	Зачет

6.4. Оценочные материалы для текущего контроля

Задания для тестирования по дисциплине для оценки сформированности компетенций (min 20, max 50 + ссылку на ЭИОС с тестами)

Ссылка на тест: https://lms2.sseu.ru/course/index.php?categoryid=514

Задание №1

Максимальное расстояние между компьютерами в локальной сети Ethernet	
Выберите один из 5 вариантов ответа:	
1)	10 км.
2)	2500 м.
3)	90 м.
4)	1000 м.
5)	500 м.

Задание №2	
Обмен информацией между компьютерными сетями, в которых действуют разные сетевые протоколы, осуществляется с использованием	
Выберите один из 5 вариантов ответа:	
1)	хост-компьютеров
2)	файл-серверов
3)	модемов
4)	шлюзов
5)	электронной почты

Задание №3	
Сколько проводов использует стандарт 100Base-T4	
Выберите один из 4 вариантов ответа:	
1)	2
2)	1
3)	4
4)	8

Задание №4	
В основе централизованной модели сертификации лежит уполномоченный орган, называемый	
Выберите один из 4 вариантов ответа:	
1)	удостоверяющим центром сертификации
2)	вышестоящим центром сертификации
3)	доверенным центром сертификации
4)	корневым центром сертификации

Задание №5	
Какое оптоволокно более толстое?	
Выберите один из 3 вариантов ответа:	
1)	Одномодовое
2)	Коаксиальное
3)	Многомодовое

Задание №6	
Какой способ реализации криптографических методов обладает максимальной скоростью обработки данных?	
Выберите один из 4 вариантов ответа:	
1)	программный

2)	аппаратный
3)	электромеханический
4)	ручной

Задание №7

Расшифруйте сообщение @-*!(-)^#*, зашифрованное с помощью шифра №2. Ответ запишите прописными буквами. Если ответ состоит из нескольких слов, запишите его пробелами, например: НОВОЕ ЗАДАНИЕ

Откр. текст	Шифр 1	Шифр 2	Откр. текст	Шифр 1	Шифр 2	Откр. текст	Шифр 1	Шифр 2
А	В	^	М	Т	№	Ч	М	∑
Б	И	@	Н	Ц	#	Ш	У	∇
В	О	)	О	.	-	Щ	Д	↑
Г	А	+	П	Ж	=	Ъ	Э	∞
Д	Щ	<	Р	Г	(	Ы	Н	⊕
Е	П	>	С	Л	?	Ь	Ю	×
Ж	К	∀	Т	Х	%	Э	Ы	ω
З	Б	♦	У	С	⊗	Ю	Ш	$
И	Ъ	*	Ф	Ь	!	Я	Е	Δ
К	пробел	♥	Х	Ч	№	пробел	Ф	∞
Л	Р	♠	Ц	З	®	.	Я	♣

Задание №8

Шифрование – это:

Выберите один из 3 вариантов ответа:

1)	процесс создания алгоритмов шифрования
2)	процесс сжатия информации
3)	процесс криптографического преобразования информации к виду, когда ее смысл полностью теряется

Задание №9

Условие, при котором в распоряжении аналитика находиться возможность получить результат зашифровки для произвольно выбранного им зашифрованного сообщения размера n используется в анализе:

Выберите один из 3 вариантов ответа:

1)	на основе только шифротекста
2)	на основе произвольно выбранного шифротекста
3)	на основе произвольно выбранного открытого текста

Задание №10

Что в криптографии называют открытым текстом?

Выберите один из 4 вариантов ответа:

1)	открытый ключ шифрования
2)	сообщение, полученное после преобразования с использованием любого шифра
3)	исходное сообщение (сообщение до шифрования)
4)	электронную цифровую подпись

Задание №11

Расшифруйте сообщение ИБЛКНАКУ, зашифрованное методом перестановки с фиксированным переводом d=6 с ключом 73825146.

Задание №12

Шифр, который заключается в перестановках структурных элементов шифруемого блока данных-битов, символов, цифр – это:

Выберите один из 3 вариантов ответа:

1)	шифр замен
2)	шифр перестановок
3)	шифр функциональных преобразований

Задание №13

Условие, при котором в распоряжении аналитика находится возможность получить результат зашифровки для произвольно выбранного им массива открытых данных размера n используется в анализе:

Выберите один из 3 вариантов ответа:

1)	на основе произвольно выбранного открытого текста
2)	на основе произвольно выбранного шифротекста
3)	правильного ответа нет

Задание №14

Как называется "исторический" шифр, в котором каждая буква исходного текста заменялась буквой, стоящей на некоторое фиксированное число мест дальше в алфавите, о применении которого имеются документальные свидетельства?

Выберите один из 4 вариантов ответа:

1)	шифр Цезаря
2)	шифр Бэббиджа
3)	шифр Маркова
4)	шифр Энигма

Задание №15

Определите ключи шифра Цезаря, если известны следующая пара открытый текст-шифротекст: ГРУША-КЛОУНЫ (исходный алфавит: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ)

Задание №16

Создание помех для нормальной работы канала передачи связи, то есть нарушение работоспособности канала связи возникает:

Выберите один из 3 вариантов ответа:

1)	со стороны законного получателя сообщения
2)	со стороны злоумышленника
3)	со стороны законного отправителя сообщения

Задание №17

Определите ключ в системе шифрования, использующий перестановку с фиксированным периодом d=5 по паре открытых и зашифрованных сообщений: ОДНА_БУКВА-_НОАДАКБВУ. Ответ запишите в виде последовательности цифр без пробелов.

Задание №18

Процесс нахождения открытого сообщения соответственно заданному закрытому при

неизвестном криптографическом преобразовании называется:

Выберите один из 3 вариантов ответа:

1)	расшифровка
2)	дешифровка
3)	шифрование

Задание №19

Расшифруйте сообщение ¦(*=%-+(^№№^, зашифрованное с помощью шифра №2. Ответ запишите прописными буквами. Если ответ состоит из нескольких слов, запишите его пробелами, например: НОВОЕ ЗАДАНИЕ

Откр. текст	Шифр 1	Шифр 2	Откр. текст	Шифр 1	Шифр 2	Откр. текст	Шифр 1	Шифр 2
А	В	^	М	Т	№	Ч	М	∑
Б	И	@	Н	Ц	#	Ш	У	∇
В	О	)	О	.	-	Щ	Д	↑
Г	А	+	П	Ж	=	Ъ	Э	ℵ
Д	Щ	<	Р	Г	(	Ы	Н	⊕
Е	П	>	С	Л	?	Ь	Ю	×
Ж	К	∀	Т	Х	%	Э	Ы	ω
З	Б	♦	У	С	⊗	Ю	Ш	$
И	Ъ	*	Ф	Ь	!	Я	Е	Δ
К	пробел	♥	Х	Ч	№	пробел	Ф	∞
Л	Р	♠	Ц	З	®	.	Я	♣

Задание №20

Как называется шифр, в котором каждый символ открытого текста заменяется некоторым, фиксированным при данном ключе символом другого алфавита?

Выберите один из 4 вариантов ответа:

1)	Шифром Цезаря
2)	Шифром одноалфавитной подстановки
3)	Шифром замены
4)	Шифром многоалфавитной подстановки

Задание №21

Как называется способ шифрования, в котором шифрование выполняется путем сложения символов исходного текста и ключа по модулю, равному числу букв в алфавите?

Выберите один из 5 вариантов ответа:

1)	Одноалфавитная подстановка
2)	Асимметричное шифрование
3)	Гаммирование
4)	Перестановка
5)	Монофоническая подстановка

Задание №22

Расшифруйте сообщение Ж.ЩО.ЩДВЕФР.Щ В, зашифрованное с помощью шифра №1. Ответ запишите прописными буквами. Если ответ состоит из нескольких слов, запишите его пробелами, например: НОВОЕ ЗАДАНИЕ

Откр. текст	Шифр 1	Шифр 2	Откр. текст	Шифр 1	Шифр 2	Откр. текст	Шифр 1	Шифр 2
А	В	^	М	Т	№	Ч	М	∑
Б	И	@	Н	Ц	#	Ш	У	∇
В	О	)	О	.	-	Щ	Д	⊺
Г	А	+	П	Ж	=	Ъ	Э	ℵ
Д	Щ	<	Р	Г	(	Ы	Н	⊕
Е	П	>	С	Л	?	Ь	Ю	×
Ж	К	∀	Т	Х	%	Э	Ы	ω
З	Б	♦	У	С	⊗	Ю	Ш	$
И	Ъ	*	Ф	Ь	!	Я	Е	Δ
К	пробел	♥	Х	Ч	№	пробел	Ф	∞
Л	Р	♠	Ц	З	®	.	Я	♣

Задание №23

Можно ли отнести слабую аутентификацию к проблемам безопасности?

Выберите один из 3 вариантов ответа:

1) в редких случаях
2) нет
3) да

Задание №24

Определите ключ в системе шифрования, использующий перестановку с фиксированным периодом d=5 по паре открытых и зашифрованных сообщений:
ОБЩИЙ_КЛЮЧ-ИЩБЙЩЮЛКЧ_. Ответ запишите в виде последовательности цифр без пробелов.

Задание №25

Известно, что при использовании шифра пропорциональной замены каждой русской букве поставлено в соответствие одно или несколько трехзначных чисел по таблице замен:

Символ	Варианты замены					Символ	Варианты замены					
А	760	128	350	201		С	800	767	105			
Б	101					Т	759	135	214			
В	210	106				У	544					
Г	351					Ф	560					
Д	129					Х	768					
Е	761	130	802	352		Ц	545					
Ж	102					Ч	215					
З	753					Ш	103					
И	762	211	131			Щ	752					
К	754	764				Ъ	561					
Л	132	354				Ы	136					
М	755	742				Ь	562					
Н	763	756	212			Э	750					
О	757	213	765	133	353	Ю	570					
П	743	766				Я	216	104				
Р	134	532				Пробел	751	769	758	801	849	035…

Расшифруйте сообщение 2118001357652152127627548011317635601331347427605452111 31. Запишите прописными русскими буквами; при необходимости для разделения слов используйте пробел.

Задание №26

Следуя принципу Кергхоффа, необходимо держать в секрете

Выберите один из 4 вариантов ответа:	
1)	Алгоритм шифрования
2)	Ключ
3)	Алгоритм шифрования и дешифрования
4)	Алгоритм дешифрования

Задание №27	
Метод, при котором для безопасности скрывается факт передачи сообщения, называется	
Выберите один из 4 вариантов ответа:	
1)	Стеганографией
2)	Хэшированием
3)	Сжатием
4)	Криптографией

Задание №28	
В каких шифрах результат шифрования очередного блока зависит только от него самого и не зависит от других блоков шифруемого массива данных?	
Выберите один из 2 вариантов ответа:	
1)	в потоковых
2)	в блочных

Задание №29	
Функция, предназначенная для выработки блока данных, используемого для модификации шифруемого блока, из инварианта и ключевого элемента называется	
Выберите один из 2 вариантов ответа:	
1)	функция шифрования шага преобразования
2)	инвариант стандартного шага шифрования

Задание №30	
Цифровая подпись обеспечивает	
Выберите один из 4 вариантов ответа:	
1)	Защиту против неправомочного доступа к данным
2)	Установление подлинности передатчика
3)	Защиту данных от несанкционированного раскрытия
4)	Защиту данных от модификации, вставки, удаления и повторной передачи информации противником

Задание №31	
В каких основных форматах существует симметричный алгоритм?	
Выберите один из 3 вариантов ответа:	
1)	потока и блока
2)	блока и строки
3)	потока и данных

Задание №32
Алиса получила электронное письмо с неизвестной ей кодировкой. Перебрав все кодировки

(кириллица, юникод, латиница), она прочитала его. Это была атака:	
Выберите один из 4 вариантов ответа:	
1)	По исходному тексту
2)	Грубой силы
3)	Статистическая
4)	По выборке исходного текста

Задание №33	
Криптография с симметричными ключами основана на использовании:	
Выберите один из 2 вариантов ответа:	
1)	одного и того же секретного ключа при зашифровании и расшифровании сообщения
2)	двух секретных ключей при зашифровании сообщения – один, при расшифровании сообщения – другой

Задание №34	
Характерная черта алгоритма Эль-Гамаля состоит в	
Выберите один из 3 вариантов ответа:	
1)	протоколе передачи подписанного сообщения, позволяющего подтверждать подлинность отправителя
2)	в точной своевременной передаче сообщения
3)	алгоритм не имеет особенностей и идентичен RSA

Задание №35	
Аутентификация бывает	
Выберите один из 5 вариантов ответа:	
1)	устойчивая
2)	все варианты правильные
3)	правильного варианта нет
4)	статическая
5)	постоянная

Задание №36	
Ограничение разглашения о схеме расположения оборонных объектов относится к сохранению	
Выберите один из 4 вариантов ответа:	
1)	готовности
2)	секретности
3)	целостности
4)	конфиденциальности

Задание №37	
Размер ключа в DES?	
Выберите один из 4 вариантов ответа:	
1)	64 бита
2)	56 бит
3)	16 байт
4)	8 бит

Задание №38	
Аппаратные и программные средства генерации случайных чисел используются в:	
Выберите один из 2 вариантов ответа:	
1)	Симметричных криптосистемах
2)	Асимметричных криптосистемах

Задание №39	
Услуга "аутентификация" обеспечивает	
Выберите один из 4 вариантов ответа:	
1)	Защиту данных от модификации, вставки, удаления и повторной передачи информации противником
2)	Защиту против неправомочного доступа к данным
3)	Защиту данных от несанкционированного раскрытия
4)	Установление подлинности объектов разного уровня

Задание №40	
Какой ключ известен только приемнику?	
Выберите один из 2 вариантов ответа:	
1)	закрытый
2)	открытый

Задание №41	
Тест Казиского позволяет	
Выберите один из 4 вариантов ответа:	
1)	Провести атаку грубой силы
2)	Найти длину ключа
3)	Сгруппировать зашифрованный текст
4)	Провести частотный анализ

Задание №42	
В каком случае построение цифровой подписи не требует наличия в системе третьего лица - арбитра, занимающегося аутентификацией?	
Выберите один из 3 вариантов ответа:	
1)	арбитр необходим всегда
2)	при шифровании с помощью симметричного алгоритма
3)	при шифровании с помощью ассимметричного алгоритма

Задание №43	
Ключевые шифры переставляют символы:	
Выберите один из 4 вариантов ответа:	
1)	Используя ключ для шифрования
2)	Используя ключ при передаче
3)	В определенных группах
4)	Исходного текста при записи, согласно ключу

Задание №44	
Конфиденциальность относится к ... безопасности	
Выберите один из 4 вариантов ответа:	
1)	методам
2)	целям
3)	механизмам
4)	услугам

Задание №45	
Аутентификацией называют	
Выберите один из 3 вариантов ответа:	
1)	процесс регистрации в системе
2)	способ защиты системы
3)	процесс распознавания и проверки подлинности заявлений о себе пользователей и процессов

Задание №46	
Частотная модуляция (ЧМ) –	
Выберите один из 3 вариантов ответа:	
1)	вид модуляции колебаний, при которой фаза несущего колебания управляется информационным сигналом
2)	модуляция, при которой незатухающие колебания изменяются по амплитуде в соответствии с модулирующими его колебаниями более низкой частоты
3)	модуляция, при которой несущая частота сигнала изменяется в соответствии с модулирующим колебанием

Задание №47	
Микроволны распространяются	
Выберите один из 2 вариантов ответа:	
1)	огибая горизонт, здания - как радиоволны
2)	по прямой линии - как свет

Задание №48	
Аналоговый сигнал – это	
Выберите один из 3 вариантов ответа:	
1)	сигнал данных полученный - путем взятия отсчетов непрерывного сигнала во времени при его преобразовании из непрерывной функции в дискретную
2)	сигнал данных, разбитый на диапазон значений непрерывной или дискретной величины на конечное число интервалов
3)	сигнал данных, у которого каждый из представляющих параметров описывается функцией времени и непрерывным множеством возможных значений

Задание №49	
Инфракрасное излучение	
Выберите один из 5 вариантов ответа:	
1)	Не проходит сквозь твердые объекты
2)	Огибает железобетонные стены

3)	Создает помехи для радиосвязи
4)	Отражается от ионосферы
5)	Плохо работает на открытом солнце

Задание №50	
Модуляция – это	
Выберите один из 3 вариантов ответа:	
1)	процесс преобразования цифровой информации в аналоговую
2)	процесс объединения информационного звукового сигнала, с частотой генератора
3)	процесс квантования модулированного сигнала

Практические задачи (min 20, max 50 + ссылку на ЭИОС с электронным изданием, если имеется)

Раздел дисциплины	**Задачи**
Информация как объект защиты	Перевести числа в десятичную систему счисления 325 246 478
Информационная безопасность	Перевести числа из десятичной системы счисления в указанную 4510=?5 2510=?6 4210=?8
Критерии оценки безопасности компьютерных систем	Перевести числа в двоичную и шестнадцатеричную системы счисления 2234 1238 5310
Криптографические средства защиты информации	Определить количество различных символов исходного текста, составить алфавит сообщения и определить длину кодовых слов. Варианты заданий 1. БАРАН КАРАБКАЛСЯ С КАРАБИНОМ 2. ТАРАКАН ПОПАЛ В КАПКАН 3. БАРАБАНЩИК БИЛ В ЯЩИК 4. КОЛОКОЛ ИЗ ВОЛОКОЛАМСКА 5. ПОЛОТЕНЦЕ ПОПАЛО В БОЛОТО 6. КОЛОБОК ПОЛОТЕНЦЕ УВОЛОК 7. ХЕРЕС ПОПАЛ НА ПЕРЕВЯЗЬ 8. МЕЛ ЕМЕЛЯ МЕЛ В МЕЛЬНИЦЕ 9. НА ЛАПУ УПАЛА КАПЛЯ ПАКЛИ 10. НЕ ПЕЙ ПЕНУ У РЕПЕЙНИКА 11. КОЛЕСИЛ СОКОЛ ОКОЛО ОКОЛИЦЫ 12. КАК ЛОМ САМ ПОЛОМАЛСЯ ПОПОЛАМ
Электронная цифровая подпись	Составить таблицу кодирования символов кодом постоянной длины. сообщения. Варианты заданий 1. БАРАН КАРАБКАЛСЯ С КАРАБИНОМ 2. ТАРАКАН ПОПАЛ В КАПКАН 3. БАРАБАНЩИК БИЛ В ЯЩИК 4. КОЛОКОЛ ИЗ ВОЛОКОЛАМСКА 5. ПОЛОТЕНЦЕ ПОПАЛО В БОЛОТО 6. КОЛОБОК ПОЛОТЕНЦЕ УВОЛОК 7. ХЕРЕС ПОПАЛ НА ПЕРЕВЯЗЬ 8. МЕЛ ЕМЕЛЯ МЕЛ В МЕЛЬНИЦЕ 9. НА ЛАПУ УПАЛА КАПЛЯ ПАКЛИ

	10. НЕ ПЕЙ ПЕНУ У РЕПЕЙНИКА 11. КОЛЕСИЛ СОКОЛ ОКОЛО ОКОЛИЦЫ 12. КАК ЛОМ САМ ПОЛОМАЛСЯ ПОПОЛАМ
Защита от копирования	Закодировать исходное сообщение полученным двоичным кодом и определить длину сообщения. Варианты заданий 1. БАРАН КАРАБКАЛСЯ С КАРАБИНОМ 2. ТАРАКАН ПОПАЛ В КАПКАН 3. БАРАБАНЩИК БИЛ В ЯЩИК 4. КОЛОКОЛ ИЗ ВОЛОКОЛАМСКА 5. ПОЛОТЕНЦЕ ПОПАЛО В БОЛОТО 6. КОЛОБОК ПОЛОТЕНЦЕ УВОЛОК 7. ХЕРЕС ПОПАЛ НА ПЕРЕВЯЗЬ 8. МЕЛ ЕМЕЛЯ МЕЛ В МЕЛЬНИЦЕ 9. НА ЛАПУ УПАЛА КАПЛЯ ПАКЛИ 10. НЕ ПЕЙ ПЕНУ У РЕПЕЙНИКА 11. КОЛЕСИЛ СОКОЛ ОКОЛО ОКОЛИЦЫ 12. КАК ЛОМ САМ ПОЛОМАЛСЯ ПОПОЛАМ
Программы с потенциально опасными последствиями	Рассчитать эффективность полученного кода постоянной длины для заданного сообщения. Варианты заданий 1. БАРАН КАРАБКАЛСЯ С КАРАБИНОМ 2. ТАРАКАН ПОПАЛ В КАПКАН 3. БАРАБАНЩИК БИЛ В ЯЩИК 4. КОЛОКОЛ ИЗ ВОЛОКОЛАМСКА 5. ПОЛОТЕНЦЕ ПОПАЛО В БОЛОТО 6. КОЛОБОК ПОЛОТЕНЦЕ УВОЛОК 7. ХЕРЕС ПОПАЛ НА ПЕРЕВЯЗЬ 8. МЕЛ ЕМЕЛЯ МЕЛ В МЕЛЬНИЦЕ 9. НА ЛАПУ УПАЛА КАПЛЯ ПАКЛИ 10. НЕ ПЕЙ ПЕНУ У РЕПЕЙНИКА 11. КОЛЕСИЛ СОКОЛ ОКОЛО ОКОЛИЦЫ 12. КАК ЛОМ САМ ПОЛОМАЛСЯ ПОПОЛАМ
Защита в интернет	Выписать исходное сообщение и составить алфавит открытого текста. 2. Составить таблицу замен символов открытого текста символами шифртекста. 3. Составить шифртекст. 4. Рассчитать частоту появления отдельных символов в открытом тексте и шифртексте. Варианты заданий для шифра Цезаря 1. БАРАН КАРАБКАЛСЯ С КАРАБИНОМ (k=4) 2. ТАРАКАН ПОПАЛ В КАПКАН (k=2) 3. БАРАБАНЩИК БИЛ В ЯЩИК (k=6) 4. КОЛОКОЛ ИЗ ВОЛОКОЛАМСКА (k=3) 5. ПОЛОТЕНЦЕ ПОПАЛО В БОЛОТО (k=5) 6. КОЛОБОК ПОЛОТЕНЦЕ УВОЛОК (k=7) 7. ХЕРЕС ПОПАЛ НА ПЕРЕВЯЗЬ (k=3) 8. МЕЛ ЕМЕЛЯ МЕЛ В МЕЛЬНИЦЕ (k=4) 9. НА ЛАПУ УПАЛА КАПЛЯ ПАКЛИ (k=7) 10. НЕ ПЕЙ ПЕНУ У РЕПЕЙНИКА (k=6) 11. КОЛЕСИЛ СОКОЛ ОКОЛО ОКОЛИЦЫ (k=5) 12. КАК ЛОМ САМ ПОЛОМАЛСЯ ПОПОЛАМ (k=2)

6.5. Оценочные материалы для промежуточной аттестации

Фонд вопросов для проведения промежуточного контроля в форме зачета

Раздел дисциплины	Вопросы
Информация как объект защиты	Прогресс информационных технологий и необходимость обеспечения информационной безопасности. 2. Основные понятия информационной безопасности. 3. Структура понятия информационная безопасность. 4. Система защиты информации и ее структура. 5. Экономическая информация как товар и объект безопасности. 6. Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии. 7. Персональные данные и их защита. 8. Информационные угрозы, их виды и причины возникновения. 9. Информационные угрозы для государства.
Информационная безопасность	10. Информационные угрозы для компании. 11. Информационные угрозы для личности (физического лица). 12. Действия и события, нарушающие информационную безопасность. 13. Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации информационных угроз. 14. Способы воздействия информационных угроз на объекты. 15. Внешние и внутренние субъекты информационных угроз. 16. Компьютерные преступления и их классификация. 17. Исторические аспекты компьютерных преступлений и современность. 18. Субъекты и причины совершения компьютерных преступлений.
Критерии оценки безопасности компьютерных систем	19. Вредоносные программы, их виды. 20. История компьютерных вирусов и современность. 21. Государственное регулирование информационной безопасности. 22. Деятельность международных организаций в сфере информационной безопасности. 23. Нормативно-правовые аспекты в области информационной безопасности в Российской Федерации. 24. Доктрина информационной безопасности России.
Криптографические средства защиты информации	25. Уголовно-правовой контроль над компьютерной преступностью в России. 26. Федеральные законы по ИБ в РФ. 27. Политика безопасности и ее принципы. 28. Фрагментарный и системный подход к защите информации. 29. Методы и средства защиты информации. 30. Организационное обеспечение ИБ.
Электронная цифровая подпись	31. Организация конфиденциального делопроизводства. 32. Комплекс организационно-технических мероприятий по обеспечению защиты информации. 33. Инженерно-техническое обеспечение компьютерной безопасности. 34. Организационно-правовой статус службы безопасности. 35. Защита информации в Интернете.
Защита от копирования	36. Электронная почта и ее защита. 37. Защита от компьютерных вирусов. 38. «Больные» мобильники и их «лечение». 39. Популярные антивирусные программы и их классификация. 40. Организация системы защиты информации экономических объектов. 41. Криптографические методы защиты информации.
Программы с потенциально	42. Этапы построения системы защиты информации. 43. Оценка эффективности инвестиций в информационную

опасными последствиями	безопасность. 44. План обеспечения непрерывной работы и восстановления функционирования автоматизированной информационной системы. 45. Управление информационной безопасности на государственном уровне. 46. Аудит ИБ автоматизированных банковских систем. 47. Электронная коммерция и ее защита. 48. Менеджмент и аудит информационной безопасности на уровне предприятия.
Защита в интернет	49. Информационная безопасность предпринимательской деятельности. 50. Обеспечение информационной безопасности должностных лиц и представителей деловых кругов.

6.6. Шкалы и критерии оценивания по формам текущего контроля и промежуточной аттестации

Шкала и критерии оценивания

Оценка	**Критерии оценивания для мероприятий контроля с применением 2-х балльной системы**
«зачтено»	ОК12з1, ОК12у1, ОК12в1, ПК29з1, ПК29у1, ПК29в1
«не зачтено»	Результаты обучения не сформированы на пороговом уровне