Документ подписан простой электронной подписью.
Информация о владельце:

ФИО: Кандрашина Елена Александровна

Должность: И.о. ректора ФГАОУ ВО «Самарский государственный экономический университет»

Дата подписания: 29.07.2025 13:15:05

Уникальный программный ключ:

2db64eb9605ce27edd3b8e8fdd32c70e0674ddd2

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

Институт Институт национальной и мировой экономики

Кафедра Региональной экономики и управления

УТВЕРЖДЕНО

Ученым советом Университета

(протокол № 10 от 22 мая 2025 г.)

РАБОЧАЯ ПРОГРАММА

Наименование дисциплины	Б1.В.ДЭ.05.01 Основы информационной безопасности
Основная профессиональная образовательная программа	38.03.04 Государственное и муниципальное управление программа Экономика и государственное управление

Квалификация (степень) выпускника Бакалавр

Содержание (рабочая программа)

Стр.

- 1 Место дисциплины в структуре ОП
- 2 Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов обучения по программе
- 3 Объем и виды учебной работы
- 4 Содержание дисциплины
- 5 Материально-техническое и учебно-методическое обеспечение дисциплины
- 6 Фонд оценочных средств по дисциплине

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

1. Место дисциплины в структуре ОП

Дисциплина Основы информационной безопасности входит в часть, формируемая участниками образовательных отношений (дисциплина по выбору) блока Б1.Дисциплины (модули)

Предшествующие дисциплины по связям компетенций: Макроэкономическое планирование и прогнозирование, Региональная экономика и управление, Маркетинг территорий, Технологии формирования имиджа и медиапланирование, Связи с общественностью в органах власти, Технологии работы в социальных сетях, Информационно -коммуникационные технологии в профессиональной деятельности

Последующие дисциплины по связям компетенций: Государственные сервисы и электронное правительство

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

Изучение дисциплины Основы информационной безопасности в образовательной программе направлено на формирование у обучающихся следующих компетенций:

Профессиональные компетенции (ПК):

ПК-3 - Способен разрабатывать и применять административный регламент при оказании государственных и муниципальных услуг

Планируемые результаты обучения по программе	Планируемые результаты обучения по дисциплине		
ПК-3	ПК-3.1: Знать:	ПК-3.2: Уметь:	ПК-3.3: Владеть (иметь навыки):
	правила разработки и утверждения административных регламентов предоставления государственных и муниципальных услуг	применять административный регламент при оказании государственных и муниципальных услуг	навыками разработки, согласования, проведение экспертизы и утверждение проектов административных регламентов

ПК-7 - Способен обеспечить защиту государственной тайны и конфиденциальной информации

Планируемые результаты обучения по программе	Планируемые результаты обучения по дисциплине		
ПК-7	ПК-7.1: Знать:	ПК-7.2: Уметь:	ПК-7.3: Владеть (иметь навыки):
	нормативно-правовую основу защиты государственной тайны и работы с конфиденциальной информацией	работать со сведениями, составляющими государственную тайну	навыками ведения секретного делопроизводства

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 7
Контактная работа, в том числе:	36.15/1
Занятия лекционного типа	18/0.5
Занятия семинарского типа	18/0.5
Индивидуальная контактная работа (ИКР)	0.15/0
Самостоятельная работа:	53.85/1.5
Промежуточная аттестация	18/0.5
Вид промежуточной аттестации:	
Зачет	Зач
Общая трудоемкость (объем части образовательной программы): Часы	108
Зачетные единицы	3

4. Содержание дисциплины

4.1. Разделы, темы дисциплины и виды занятий:

Тематический план дисциплины Основы информационной безопасности 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	ИКР	ГКР		
Практич. занятия							
1.	Введение в основы информационной безопасности.	8	8	0,075		20	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3
2.	Глобальные сети и Интернет Облачные и мобильные технологии с точки зрения безопасности.	10	10	0,075		33,85	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3
	Контроль	18					
	Итого	18	18	0.15		53.85	

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.	Основные понятия информационной безопасности.	лекция	Понятие национальной и информационной безопасности РФ.
		лекция	Государственная информационная политика. Государственная тайна.
		лекция	Место информационной безопасности экономических систем в национальной

		лекция	безопасности страны.
2.	Нормативы и Стандарты.	лекция	Законодательная база информационной безопасности.
		лекция	Доктрина информационной безопасности РФ.
		лекция	
		лекция	
		лекция	

*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.	Основные понятия информационной безопасности.	практическое занятие	Освоение основных понятий и терминологии информационной безопасности;
		практическое занятие	- вирусные атаки и защита от них;
		практическое занятие	- изучение организационно-административных и технических методов и средств
		практическое занятие	защиты информации;
2.	Нормативы и Стандарты.	практическое занятие	- стандарты в области информационной безопасности;
		практическое занятие	- лабораторная работа «Шифрование данных».
		практическое занятие	
		практическое занятие	
		практическое занятие	

** 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.	Тема 1 Основные понятия информационной безопасности.	- подготовка доклада - подготовка электронной презентации - тестирование

	Нормативы и стандарты	
2.	Тема 2 Угрозы. Методы и средства защиты Тема 3 Безопасность автоматизированных систем	- подготовка доклада - подготовка электронной презентации - 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

1. Нестеров С.А. Основы информационной безопасности: учебное пособие. – Лань, 2019. – 324 с. – Баранова Е.К., Бабаш А.В. Основы информационной безопасности: учебник. – ИНФРА-М, 2019. – 202 с.

Дополнительная литература

1. Галатенко В.А. Основы информационной безопасности: учебное пособие. – Интернет-Университет Информационных Технологий, 2010. – 205 с. – Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов Основы информационной безопасности: учебное пособие. – Горячая линия – Телеком, 2006. – 544 с. – Е.В. Вострецова Основы информационной безопасности: учебное пособие Издательство Урал.ун-та 2019 г., 204 с. – В. В. Бондарев Введение в информационную безопасность автоматизированных систем: учебное пособие. – Издательство МГГУ им. Н. Э. Баумана, 2016. – 250 с.

5.2. Перечень лицензионного программного обеспечения

1. Astra Linux Special Edition «Смоленск», «Орел»; РедОС ; ОС "Альт Рабочая станция" 10; ОС "Альт Образование" 10
2. МойОфис Стандартный 2, МойОфис Образование, Р7-Офис Профессиональный, МойОфис Стандартный 3, МойОфис Профессиональный 3

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/>)
3. Профессиональная база данных «Финансово-экономические показатели Российской Федерации» (Официальный сайт Министерства финансов РФ - <https://www.minfin.ru/ru/>)
4. Профессиональная база данных «Официальная статистика» (Официальный сайт Федеральной службы государственной статистики - <http://www.gks.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 Мультимедийный проектор Доска
---	--

	Экран
Учебные аудитории для проведения практических занятий (занятий семинарского типа)	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Учебные аудитории для групповых и индивидуальных консультаций	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Учебные аудитории для текущего контроля и промежуточной аттестации	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Помещения для самостоятельной работы	Комплекты ученической мебели Мультимедийный 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

5.6 Лаборатории и лабораторное оборудование

6. Фонд оценочных средств по дисциплине Основы информационной безопасности:

6.1. Контрольные мероприятия по дисциплине

Вид контроля	Форма контроля	Отметить нужное знаком « + »
Текущий контроль	Оценка докладов	+
	Устный/письменный опрос	+
	Тестирование	+
	Практические задачи	+
Промежуточный контроль	Зачет	+

Порядок проведения мероприятий текущего и промежуточного контроля определяется Методическими указаниями по основной профессиональной образовательной программе высшего образования; Положением о балльно-рейтинговой системе оценки успеваемости обучающихся по основным образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в федеральном государственном автономном образовательном учреждении высшего образования «Самарский государственный экономический университет».

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

Профессиональные компетенции (ПК):

ПК-3 - Способен разрабатывать и применять административный регламент при оказании государственных и муниципальных услуг

Планируемые результаты обучения по программе	Планируемые результаты обучения по дисциплине		
	ПК-3.1: Знать:	ПК-3.2: Уметь:	ПК-3.3: Владеть (иметь навыки):
	правила разработки и утверждения административных регламентов предоставления государственных и муниципальных услуг	применять административный регламент при оказании государственных и муниципальных услуг	навыками разработки, согласования, проведение экспертизы и утверждение проектов административных регламентов
Пороговый	Порядок разработки и утверждения административных регламентов предоставления государственных и муниципальных услуг	Применять отдельные процедуры административного регламента при оказании государственных и муниципальных услуг	Анализа административных регламентов при оказании государственных и муниципальных услуг
Стандартный (в дополнение к пороговому)	Федеральные законы, нормативно-правовые акты Президента Российской Федерации и Правительства Российской Федерации, а также единый стандарт предоставления государственной услуги (при его наличии) в соответствии с которыми применяется административный регламент при оказании государственных и муниципальных услуг	Комплексно принять административные регламенты оказания государственных и муниципальных услуг с учетом принципа клиентоцентричности	Разработки и утверждения новых административных регламентов при оказании государственных и муниципальных услуг
Повышенный (в дополнение к пороговому, стандартному)	Порядок экспертизы и утверждения проектов административных регламентов предоставления государственных и муниципальных услуг	Доработать административные регламенты при оказании государственных и муниципальных услуг по результатам тестирования применения регламента	Согласования и проведения экспертизы административных регламентов при оказании государственных и муниципальных услуг

ПК-7 - Способен обеспечить защиту государственной тайны и конфиденциальной информации

Планируемые результаты обучения по программе	Планируемые результаты обучения по дисциплине		
	ПК-7.1: Знать:	ПК-7.2: Уметь:	ПК-7.3: Владеть (иметь навыки):
	нормативно-правовую основу защиты государственной тайны и работы с конфиденциальной информацией	работать со сведениями, составляющими государственную тайну	навыками ведения секретного делопроизводства
Пороговый	Основные положения законодательства о защите государственной тайны и конфиденциальной информации	Относить сведения к государственной тайне	Технического обеспечения работы с документами, учета и хранения документов и дел
Стандартный (в дополнение к пороговому)	Требования к организации защиты государственной тайны	Определять степень секретности документов	Организации секретного документооборота организации
Повышенный (в дополнение к пороговому, стандартному)	Методы выявления возможных каналов несанкционированного доступа к сведениям	Применять технологии и средства обеспечения сохранности сведений, составляющих государственную тайну	Проведения служебных расследований по фактам нарушения режима секретности

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.	Введение в основы информационной безопасности	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3	Тестирование Лабораторные работы	Зачет
2.	Глобальная безопасность информации	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3	Тестирование Лабораторные работы	Зачет

6.4. Оценочные материалы для текущего контроля

Примерная тематика докладов

Раздел дисциплины	Темы
Безопасность в общем смысле.	1 Виды защищаемой информации мероприятия по управлению доступом к информации. 2 Виды паразитных связей и наводок, характерные для любых радиоэлектронных средств и проводов, соединяющих их кабелей.

	<p>3 Методы несанкционированного доступа к информации.</p> <p>4 Основными способами привлечения сотрудников государственных и коммерческих структур, имеющих доступ к интересующей информации.</p> <p>5 Каналы утечки информации. Технические каналы утечки</p> <p>6 Защита личности как носителя информации.</p> <p>7 Системный подход к защите информации.</p> <p>8 Этапы проектирования системы защиты информации.</p> <p>9 Угрозы сохранности данных в компьютере случайного характера.</p> <p>10 Классификация вирусов и антивирусных программ.</p> <p>11 Компьютерная преступность. Виды преступной деятельности.</p> <p>12 Криптографическая защита информации (основные понятия).</p> <p>Методы шифрования данных.</p> <p>13 Проблемы региональной информационной безопасности.</p> <p>14 Правовые, организационно-технические и экономические методы обеспечения информационной безопасности.</p> <p>15 Компьютерная система как объект информационной безопасности.</p> <p>16 Особенности обеспечения информационной безопасности в различных сферах общественной жизни.</p>

Вопросы для устного/письменного опроса

Раздел дисциплины	Вопросы

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

Тест 1

- 1 Информационная безопасность и ее основные компоненты.
- 2 Вирусные атаки и защита от них.
- 3 Сформировать открытый и секретный ключ в системе RSA ($P=3$, $Q=5$).
- 4 Зашифровать сообщение (4,8) с помощью криптосистемы Хилла (модуль равен 26, матрица

Тест 2

- 1 Механизмы информационной безопасности.
- 2 Стандарты в области информационной безопасности.
- 3 Зашифровать сообщение $x=3$ в системе RSA ($P=5$, $Q=7$) с помощью ключа $e=5$.
- 4 Расшифровать сообщение (4,8) с помощью криптосистемы Хилла (модуль равен 26, матрица

Тест 3

- 1 Политика информационной безопасности.
- 2 Уровни информационной безопасности.
- 3 Расшифровать сообщение $x=4$ в системе RSA ($P=5$, $Q=7$) с помощью ключа $d=5$.
- 4 Зашифровать сообщение «информация» с помощью шифра Цезаря.

Тест 4

- 1 Принципы криптографической защиты информации.
- 2 Угрозы и способы обеспечения информационной безопасности.
- 3 Найти и объяснить, используемые в операционной системе Windows средства обеспечения конфиденциальности информации.

4 Закодировать с помощью метода Хаффмена слово «стандарт»

Тест 5

1.Классификация криптосистем.

2.Электронная подпись, правовой и технический аспекты.

3 Найти и объяснить, используемые в операционной системе Windows средства обеспечения целостности информации.

4 Закодировать с помощью метода Фано слово «стандарт».

Тест 6

1 Классификация компьютерных вирусов.

2 Способы распространения вирусов.

3 Троянские программы и их особенности.

4 Лечение компьютерных вирусов. Методы борьбы с ними.

5 Классификация антивирусных программ.

Тест 7

1.Классификация компьютерных сетей с точки зрения безопасности.

2.Системы управления доступом. Сервера Kerberos и Active Directory.

3 Уязвимости компьютерных сетей. DDOS атаки. Эскалация привилегий. Ошибки в ПО. Человеческий фактор.

4 Основные способы взлома

6.5. Оценочные материалы для промежуточной аттестации

Фонд вопросов для проведения промежуточного контроля в форме зачета

Раздел дисциплины	Вопросы
Основы информационной безопасности	1 Информационная безопасность и ее основные компоненты. 2 Административный и процедурный уровни информационной безопасности. 3 Механизмы информационной безопасности. 4 Политика информационной безопасности. 5 Классификация атак, уровни безопасности. 6 Уязвимости и политика информационной безопасности. 7 Угрозы и способы обеспечения информационной безопасности 8 Стандарты в области информационной безопасности 9 Типы кодов, обнаруживающих и исправляющих ошибки, примеры. 10 Принципы криптографической защиты информации. 11 Симметричные и асимметричные криптосистемы. 12 Проблемы идентификации и проверки подлинности. 13 Электронная подпись, правовой и технический аспекты. 14 Межсетевые экраны и их предназначение. 15 Вирусные атаки и защита от них. 16 Классы моделей политик безопасности. 17 Основные положения государственной политики информационной безопасности, мероприятия по их реализации. 18 Понятие «информационная война». 19 Защита от деструктивного воздействия информации. 20 Информация ограниченного доступа. 21 Задачи информационной защиты в финансовой сфере. 22 Задачи информационной защиты в сфере предоставления услуг связи. 23 Организационно-распорядительные меры информационной защиты. 24 Специфика объектов информационной защиты.

	25 Модель комплексной информационной защиты и ее элементы. 26 Модель информационной защиты каналов связи. 27 Формы и методы защиты признаковой информации.

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»	ПК-3, ПК-7
«не зачтено»	Результаты обучения не сформированы на пороговом уровне