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

Институт Экономики предприятий

Кафедра Цифровых технологий и решений

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

РАБОЧАЯ ПРОГРАММА

Наименование дисциплины Б1.В.ДВ.11.01 Основы информационной безопасности

Основная профессиональная образовательная программа Направление 09.03.03 ПРИКЛАДНАЯ ИНФОРМАТИКА программа "Прикладная информатика в электронной экономике"

Методический отдел УМУ
«10» 03 2020г.
_____ / Каланчева М.А./

Научная библиотека СГЭУ
«10» 03 2020г.
_____ / Гуреева /

Рассмотрено к утверждению
на заседании кафедры Цифровых технологий и решений
(протокол № 8 от 05.03.2020г.)
Зав. кафедрой_____ / Погорелова Е.В./

Квалификация (степень) выпускника бакалавр

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 Основы информационной безопасности входит в вариативную часть (дисциплина по выбору) блока Б1.Дисциплины (модули)

Предшествующие дисциплины по связям компетенций: Право, Предпринимательское право, Коммерческое право, Базы данных, Администрирование баз данных, Системная архитектура информационных систем, Технологии управления знаниями, Моделирование бизнес-процессов

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:

Общекультурные компетенции (ОК):

ОК-4 - способностью использовать основы правовых знаний в различных сферах деятельности

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
ОК-4	**Знать**	**Уметь**	**Владеть**
	основы правовых знаний в различных сферах деятельности	использовать основы правовых знаний в различных сферах деятельности	способностью использовать основы правовых знаний в различных сферах деятельности

Профессиональные компетенции (ПК):

ПК-4 - способностью документировать процессы создания информационных систем на стадиях жизненного цикла

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
ПК-4	**Знать**	**Уметь**	**Владеть**
	процессы создания информационных систем на стадиях жизненного цикла	документировать процессы создания информационных систем на стадиях жизненного цикла	способностью документировать процессы создания информационных систем на стадиях жизненного цикла

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 8
Контактная работа, в том числе:	65.15/1.81
Занятия лекционного типа	32/0.89
Занятия семинарского типа	32/0.89
Индивидуальная контактная работа (ИКР)	0.15/0
Групповая контактная работа (ГКР)	1/0.03
Самостоятельная работа, в том числе:	23.85/0.66
Промежуточная аттестация	19/0.53
Вид промежуточной аттестации: Зачет	Зач
Общая трудоемкость (объем части образовательной программы): Часы Зачетные единицы	108 3

заочная форма

Виды учебной работы	Всего час/ з.е.
	Сем 9
Контактная работа, в том числе:	13.15/0.37
Занятия лекционного типа	4/0.11
Занятия семинарского типа	8/0.22
Индивидуальная контактная работа (ИКР)	0.15/0
Групповая контактная работа (ГКР)	1/0.03
Самостоятельная работа, в том числе:	91.85/2.55
Промежуточная аттестация	3/0.08
Вид промежуточной аттестации: Зачет	Зач
Общая трудоемкость (объем части образовательной программы): Часы Зачетные единицы	108 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: Практич. занятия	ИКР	ГКР		
1.	Основные понятия и определения информационной безопасности	10	10			10	ОК-4з1,ОК-4з2, ОК-4у1, ОК-4у2, ОК-4в1, ОК-4в2, ПК-4з1, ПК-4з2, ПК-4у1, ПК-4у2, ПК-4в1, ПК-4в2
2.	Направления обеспечения информационной безопасности. Правовые основы обеспечения защиты информации	22	22			13,95	ОК-4з1,ОК-4з2, ОК-4у1, ОК-4у2, ОК-4в1, ОК-4в2, ПК-4з1, ПК-4з2, ПК-4у1, ПК-4у2, ПК-4в1, ПК-4в2
	Контроль	19					
	Итого	**32**	**32**	**0.15**	**1**	**23.85**	

заочная форма

№ 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.	Основные понятия и определения информационной безопасности	2	4			40	ОК-4з1,ОК-4з2, ОК-4у1, ОК-4у2, ОК-4в1, ОК-4в2, ПК-4з1, ПК-4з2, ПК-4у1, ПК-4у2,

							ПК-4в1, ПК-4в2
2.	Направления обеспечения информационной безопасности. Правовые основы обеспечения защиты информации	2	4			51,85	ОК-4з1,ОК-4з2, ОК-4у1, ОК-4у2, ОК-4в1, ОК-4в2, ПК-4з1, ПК-4з2, ПК-4у1, ПК-4у2, ПК-4в1, ПК-4в2
	Контроль	3					
	Итого	**4**	**8**	0.15	1	**91.85**	

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 и определения информационной безопасности	лекция	Основные понятия и определения информационной безопасности.
		лекция	Угрозы. Классификация угроз информационной безопасности
		лекция	Методы нарушения конфиденциальности, целостности и доступности информации
2.	Направления обеспечения информационной безопасности. Правовые основы обеспечения защиты информации	лекция	Направления обеспечения информационной безопасности.
		лекция	Правовые основы обеспечения защиты информации.
		лекция	Стандарты, используемые при создании систем информационной безопасности.
		лекция	Архитектура систем защиты информации. Функции защиты информации.
		лекция	Информационная безопасность автоматизированных информационных систем.

*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 и определения информационной безопасности	практическое занятие	Основные понятия и определения информационной безопасности.
		практическое занятие	Угрозы. Классификация угроз информационной безопасности

		практическое занятие	Методы нарушения конфиденциальности, целостности и доступности информации
2.	Направления обеспечения информационной безопасности. Правовые основы обеспечения защиты информации	практическое занятие	Направления обеспечения информационной безопасности.
		практическое занятие	Правовые основы обеспечения защиты информации.
		практическое занятие	Стандарты, используемые при создании систем информационной безопасности.
		практическое занятие	Архитектура систем защиты информации. Функции защиты информации.
		практическое занятие	Информационная безопасность автоматизированных информационных систем.

** 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.	Основные понятия и определения информационной безопасности	- подготовка доклада - подготовка электронной презентации - тестирование
2.	Направления обеспечения информационной безопасности. Правовые основы обеспечения защиты информации	- 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. Богатырев, В. А. Информационные системы и технологии. Теория надежности : учебное пособие для вузов / В. А. Богатырев. — Москва: Издательство Юрайт, 2020. — 318 с. — (Высшее образование). — ISBN 978-5-534-00475-5. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/451108

Дополнительная литература

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2020. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450371

2. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/454453

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)

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. Профессиональная база данных «Финансово-экономические показатели Российской Федерации» (Официальный сайт Министерства финансов РФ - https://www.minfin.ru/ru/)

3. 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 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

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 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	-
	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 29.04.2020 г.

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

Общекультурные компетенции (ОК):

ОК-4 - способностью использовать основы правовых знаний в различных сферах деятельности

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
	Знать	Уметь	Владеть (иметь навыки)
Пороговый	ОК-4з1 Знать: основы правовых знаний в отдельных сферах деятельности	ОК-4у1 Уметь: использовать основы правовых знаний в отдельных сферах деятельности	ОК-4в1 Владеть: способностью использовать основы правовых знаний в отдельных сферах деятельности
Повышенный	ОК-4з2 Знать: основы правовых знаний в различных сферах деятельности	ОК-4у2 Уметь: использовать основы правовых знаний в различных сферах деятельности	ОК-4в2 Владеть: способностью использовать основы правовых знаний в различных сферах деятельности

Профессиональные компетенции (ПК):

ПК-4 - способностью документировать процессы создания информационных систем на стадиях жизненного цикла

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
	Знать	Уметь	Владеть (иметь навыки)
Пороговый	ПК-4з1 Знать: процессы создания информационных систем на отдельных стадиях жизненного цикла	ПК-4у1 Уметь: документировать процессы создания информационных систем на отдельных стадиях жизненного цикла	ПК-4в1 Владеть: способностью документировать процессы создания информационных систем на отдельных стадиях жизненного цикла
Повышенный	ПК-4з2 Знать: процессы создания информационных систем на стадиях жизненного цикла	ПК-4у2 Уметь: документировать процессы создания информационных систем на стадиях жизненного цикла	ПК-4в2 Владеть: способностью документировать процессы создания информационных систем на стадиях жизненного цикла

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.	Основные понятия и определения информационной безопасности	ОК-4з1,ОК-4з2, ОК-4у1, ОК-4у2, ОК-4в1, ОК-4в2, ПК-4з1, ПК-4з2, ПК-4у1, ПК-4у2, ПК-4в1, ПК-4в2	Оценка докладов Тестирование	зачет
2.	Направления обеспечения информационной безопасности. Правовые основы обеспечения защиты информации	ОК-4з1,ОК-4з2, ОК-4у1, ОК-4у2, ОК-4в1, ОК-4в2, ПК-4з1, ПК-4з2, ПК-4у1, ПК-4у2, ПК-4в1, ПК-4в2	Оценка докладов Тестирование	зачет

6.4.Оценочные материалы для текущего контроля

Примерная тематика докладов

Раздел дисциплины	**Темы**
Основные понятия и определения информационной безопасности	1. Классификация и свойства информации. 2. Основные задачи организационно-управленческой деятельности в сфере информационной безопасности. 3. Информация как объект юридической защиты. 4. Структура и функции службы обеспечения защиты ИС на

	предприятии. 5. Задачи, роли и методы, используемые на различных уровнях организационной работы в сфере информационной безопасности. 6. Управление информационной безопасностью на предприятии. 7. Деятельность международных организаций в сфере информационной безопасности. 8. Методология организационного обеспечения информационной безопасности на уровне крупных поставщиков информационных систем.
Направления обеспечения информационной безопасности. Правовые основы обеспечения защиты информации	1. Менеджмент информационной безопасности на уровне предприятия: основные направления и структура политики безопасности. 2. Формирование политики информационной безопасности на предприятии. 3. Использование программных средств для поддержки аудита качества и надежности защиты ИС. 4. Организационная структура и персонал службы информационной безопасности на предприятии. 5. Аудит состояния информационной безопасности на предприятии. 6. Политика ИБ предприятия.

Задания для тестирования по дисциплине для оценки сформированности компетенций https://lms2.sseu.ru/course/index.php?categoryid=514

К правовым методам, обеспечивающим информационную безопасность, относятся:
Разработка аппаратных средств обеспечения правовых данных
Разработка и установка во всех компьютерных правовых сетях журналов учета действий
Разработка и конкретизация правовых нормативных актов обеспечения безопасности

Основными источниками угроз информационной безопасности являются все указанное в списке:
Хищение жестких дисков, подключение к сети, инсайдерство
Перехват данных, хищение данных, изменение архитектуры системы
Хищение данных, подкуп системных администраторов, нарушение регламента работы

Виды информационной безопасности:
Персональная, корпоративная, государственная
Клиентская, серверная, сетевая
Локальная, глобальная, смешанная

Цели информационной безопасности – своевременное обнаружение, предупреждение:
несанкционированного доступа, воздействия в сети
инсайдерства в организации
чрезвычайных ситуаций

Основные объекты информационной безопасности:
Компьютерные сети, базы данных
Информационные системы, психологическое состояние пользователей
Бизнес-ориентированные, коммерческие системы

Основными рисками информационной безопасности являются:
Искажение, уменьшение объема, перекодировка информации
Техническое вмешательство, выведение из строя оборудования сети
Потеря, искажение, утечка информации

К основным принципам обеспечения информационной безопасности относится:
Экономической эффективности системы безопасности
Многоплатформенной реализации системы
Усиления защищенности всех звеньев системы

Основными субъектами информационной безопасности являются:
руководители, менеджеры, администраторы компаний
органы права, государства, бизнеса
сетевые базы данных, фаерволлы

К основным функциям системы безопасности можно отнести все перечисленное:
Установление регламента, аудит системы, выявление рисков
Установка новых офисных приложений, смена хостинг-компании
Внедрение аутентификации, проверки контактных данных пользователей
тест

Принципом информационной безопасности является принцип недопущения:
Неоправданных ограничений при работе в сети (системе)
Рисков безопасности сети, системы
Презумпции секретности

Принципом политики информационной безопасности является принцип:
Невозможности миновать защитные средства сети (системы)
Усиления основного звена сети, системы
Полного блокирования доступа при риск-ситуациях

Принципом политики информационной безопасности является принцип:
Усиления защищенности самого незащищенного звена сети (системы)
Перехода в безопасное состояние работы сети, системы
Полного доступа пользователей ко всем ресурсам сети, системы

Принципом политики информационной безопасности является принцип:
Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
Одноуровневой защиты сети, системы
Совместимых, однотипных программно-технических средств сети, системы

К основным типам средств воздействия на компьютерную сеть относится:
Компьютерный сбой
Логические закладки («мины»)
Аварийное отключение питания

Когда получен спам по e-mail с приложенным файлом, следует:
Прочитать приложение, если оно не содержит ничего ценного – удалить
Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
Удалить письмо с приложением, не раскрывая (не читая) его

Принцип Кирхгофа:
Секретность ключа определена секретностью открытого сообщения
Секретность информации определена скоростью передачи данных
Секретность закрытого сообщения определяется секретностью ключа

ЭЦП – это:
Электронно-цифровой преобразователь
Электронно-цифровая подпись
Электронно-цифровой процессор

Наиболее распространены угрозы информационной безопасности корпоративной системы:
Покупка нелицензионного ПО
Ошибки эксплуатации и неумышленного изменения режима работы системы
Сознательного внедрения сетевых вирусов

Наиболее распространены угрозы информационной безопасности сети:

Распределенный доступ клиент, отказ оборудования
Моральный износ сети, инсайдерство
Сбой (отказ) оборудования, нелегальное копирование данных
Т**ест**

Наиболее распространены средства воздействия на сеть офиса:
Слабый трафик, информационный обман, вирусы в интернет
Вирусы в сети, логические мины (закладки), информационный перехват
Компьютерные сбои, изменение администрирования, топологии

Утечкой информации в системе называется ситуация, характеризуемая:
Потерей данных в системе
Изменением формы информации
Изменением содержания информации

Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
Целостность
Доступность
Актуальность

Угроза информационной системе (компьютерной сети) – это:
Вероятное событие
Детерминированное (всегда определенное) событие
Событие, происходящее периодически

Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
Регламентированной
Правовой
Защищаемой

Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:
Программные, технические, организационные, технологические
Серверные, клиентские, спутниковые, наземные
Личные, корпоративные, социальные, национальные

Окончательно, ответственность за защищенность данных в компьютерной сети несет:
Владелец сети
Администратор сети
Пользователь сети

Политика безопасности в системе (сети) – это комплекс:
Руководств, требований обеспечения необходимого уровня безопасности
Инструкций, алгоритмов поведения пользователя в сети
Нормы информационного права, соблюдаемые в сети

Наиболее важным при реализации защитных мер политики безопасности является:
Аудит, анализ затрат на проведение защитных мер
Аудит, анализ безопасности
Аудит, анализ уязвимостей, риск-ситуаций

6.5. Оценочные материалы для промежуточной аттестации

Фонд вопросов для проведения промежуточного контроля в форме зачета

Раздел дисциплины	Вопросы
Основные понятия и определения информационной безопасности	1. Понятие информационной безопасности, информационной системы, видов информации. 2. Понятие угрозы. Виды угроз. Источники угроз. 3. Характер происхождения угроз: умышленные факторы, естественные факторы.

	4. Защита информации на уровне предприятия (организации). 5. Организационно-правовое обеспечение информационной безопасности ИС. 6. Виды технических средств защиты информационных систем. 7. Защита информации от утечки по визуально-оптическим каналам, акустическим каналам и электромагнитным каналам. 8. Основные организационно-правовые документы по организационному обеспечению комплексной информационной безопасности предприятия. 9. Принципы организации и функционирования системы информационной безопасности предприятия (фирмы); 10. Направления деятельности службы информационной безопасности; 11. Основные функции и задачи по обеспечению информационной безопасности предприятия (фирмы)
Направления обеспечения информационной безопасности. Правовые основы обеспечения защиты информации	1. Основные задачи организационно-управленческой деятельности в сфере информационной безопасности. 2. Структура и функции службы обеспечения защиты ИС на предприятии. 3. Задачи, роли и методы, используемые на различных уровнях организационной работы 4. в сфере информационной безопасности. 5. Методология организационного обеспечения информационной безопасности на уровне крупных поставщиков информационных систем. 6. Менеджмент информационной безопасности на уровне предприятия: основные направления и структура политики безопасности. 7. Аудит состояния информационной безопасности на предприятии. 8. Формирование политики информационной безопасности на предприятии. 9. Задачи, роли и методы, используемые на различных уровнях организационной работы в сфере информационной безопасности. 10. Управление информационной безопасностью на предприятии. 11. Источники конфиденциальной информации. 12. Организационные каналы обмена и передачи информации. 13. Виды информации. 14. Понятие тайны. 15. Свойства информации. 16. Классификация носителей информации. 17. Цели защиты информации. 18. Виды технических каналов утечки информации 19. Электромагнитный канал утечки 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»	ОК-4з1, ОК-4у1, ОК-4в1, ПК-4з1, ПК-4у1, ПК-4в1,
«не зачтено»	Результаты обучения не сформированы на пороговом уровне