



КГУ

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
Федеральное государственное бюджетное образовательное  
учреждение высшего образования  
«КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭНЕРГЕТИЧЕСКИЙ УНИВЕРСИТЕТ»  
(ФГБОУ ВО «КГУ»)

АКТУАЛИЗИРОВАНО  
Решением Ученого совета ИЦТЭ КГУ  
Протокол №7 от 19.03.2024

УТВЕРЖДАЮ

Директор Института цифровых  
технологий и экономики

\_\_\_\_\_ Э.И. Беляев

«30» мая 2023 г.

## РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

### Б1.В.ДЭ.01.01.01 Информационная безопасность в корпоративных информационных системах

Направление подготовки	09.04.03 Прикладная информатика
Направленность (профиль)	Интеллектуальные и информационные системы
Квалификация	Магистр
Форма обучения	Очная

Программу разработал(и):

Наименование кафедры	Должность, уч. степень, уч. звание	ФИО разработчика
ИТИС	Доцент, к.т.н.	Исмагилов И.Р.

Согласование	Наименование подразделения	Дата	№ протокола	Подпись
Одобрена	ИТИС	27.04.23	3	Зав.каф., д.п.н., доц. Торкунова Ю.В.
Согласована	Учебно-методический совет ИЦТЭ	30.05.23	7	Директор, к.т.н., Беляев Э.И.
Одобрена	Ученый совет ИЦТЭ	30.05.23	9	Директор, к.т.н., Беляев Э.И.

## **1. Цель, задачи и планируемые результаты обучения по дисциплине**

Целью дисциплины «Информационная безопасность в корпоративных информационных системах» является получение знаний по основам управления информационной безопасностью в рамках жизненного цикла корпоративных информационных систем. Необходимость в получении таких знаний определяется тем, что магистранты должны иметь четкое понимание предметной области, которой они будут заниматься при формировании и реализации требований по информационной безопасности к корпоративным информационным системам.

В результате освоения данной дисциплины магистрант приобретает знания, умения и навыки, обеспечивающие достижение целей профессиональной подготовки и профессиональными компетенциями, позволяющими ему быть востребованным на рынке труда и в обществе. Дисциплина помогает развитию у студентов способности самостоятельно мыслить, логически выстраивать свои умозаключения, корректировать их и делать выводы по ним; способности к самообучению, умения публично выступать, представлять, обосновывать и отстаивать собственные заключения и делать выводы; работать в команде и следовать кодексу профессиональной этики. Данная дисциплина поможет будущим специалистам понять особенности этапов управления информационной безопасностью, освоить соответствующие технологии и методики, получить основные сведения о необходимых компетенциях, которыми должны обладать специалисты при создании требований к системам обеспечения информационной безопасности, управлении рисками информационной безопасности, составить общее представление о характере их работы в этом направлении.

Изучение данного курса позволит магистрам заниматься риск-менеджментом в области информационной безопасности, готовить техническое задание на системы обеспечения информационной безопасности.

Задачи дисциплины:

- формирование у будущих специалистов знаний и навыков применения нормативной и методической базы в области информационной безопасности
- овладение стандартами, а также методами и приемами оценки рисков информационной безопасности для корпоративных информационных систем
- приобретение знаний и практических навыков деятельности по применению современных технологий для сохранения и эффективного использования информационных ресурсов, обеспечения надежного функционирования корпоративных информационных систем и предоставляемых ими услуг.

Компетенции, формируемые у обучающихся, запланированные результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения по дисциплине (знать, уметь, владеть)
<b>Профессиональные компетенции (ПК)</b>		
ПК- 2 Способен к проектированию архитектуры ИС, автоматизации и информатизации решения прикладных задач предприятий и организаций	ПК 2.1 Проектирует архитектуру ИС предприятий и организаций в прикладной области с учетом требований заказчика	<p>знать:</p> <ul style="list-style-type: none"> <li>- З<sub>1</sub> архитектуру информационных систем предприятий и организаций;</li> </ul> <p>уметь:</p> <ul style="list-style-type: none"> <li>- У<sub>1</sub> выбирать методологию и технологию проектирования информационных систем;</li> </ul> <p>владеть:</p> <ul style="list-style-type: none"> <li>- В<sub>1</sub> Методами построения различных типов информационных систем.</li> </ul>
	ПК 2.2 Применяет современные методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания ИС	<p>знать:</p> <ul style="list-style-type: none"> <li>- З<sub>1</sub> современные методы и инструментальные средства прикладной информатики для автоматизации и решения профессиональных задач;</li> </ul> <p>уметь:</p> <ul style="list-style-type: none"> <li>- У<sub>1</sub> обосновывать выбор современных методов и инструментальных средств прикладной информатики для автоматизации и решения профессиональных задач;</li> </ul> <p>владеть:</p> <ul style="list-style-type: none"> <li>- В<sub>1</sub> навыками применения современных методов и инструментальных средств прикладной информатики для автоматизации и решения профессиональных задач.</li> </ul>

## 2. Место дисциплины в структуре ОПОП

Дисциплина Информационная безопасность в корпоративных информационных системах относится к части учебного плана, формируемой участниками образовательных отношений по направлению подготовки 09.04.03 Прикладная информатика.

Код компетенции	Предшествующие дисциплины (модули), практики, НИР, др.	Последующие дисциплины (модули), практики, НИР, др. <sup>1</sup>
ОПК-6.1; ОПК-6.2	Информационное общество и проблемы прикладной информатики	
ОПК-2.1; ОПК-2.2; ОПК-3.1; ОПК-3.2; ОПК-5.1; ОПК-5.2;		Производственная практика (технологическая)

ОПК-6.1; ОПК-6.2; ОПК-7.1; ОПК-7.2; ОПК-8.1; ОПК-8.2; ОПК-8.3		
ПК-1.1; ПК-1.2; ПК-1.3; ПК-2.1; ПК-2.2		Производственная практика (преддипломная)

Для освоения дисциплины обучающийся должен:

**Знать:**

- архитектуру информационных систем предприятий и организаций;
- основные законодательные акты РФ в информационной сфере;
- структуру локальных и глобальных компьютерных сетей
- характеристики технических и программных средств реализации информационных технологий.

**Уметь:**

- выбирать методологию и технологию проектирования информационных систем;
- проводить сравнительный анализ и выбор информационных технологий для решения прикладных задач;
- использовать ресурсы различных типов информационных систем для обработки информации.

**Владеть:**

- навыками разработки технологической документации, использования функциональных и технологических стандартов;
- методами построения математических моделей типовых задач; методами поиска и обмена информацией в глобальных и локальных компьютерных сетях.

### 3. Структура и содержание дисциплины

#### 3.1. Структура дисциплины

Общая трудоемкость дисциплины составляет 6 зачетных единицы (ЗЕ), всего 216 часов, из которых 69 часов составляет контактная работа обучающегося с преподавателем (занятия лекционного типа 32 час., занятия семинарского типа (практические, лабораторные работы) – 32 час., групповые и индивидуальные консультации 2 час., прием экзамена (КПА) – 1 час., самостоятельная работа обучающегося 112 час, контроль самостоятельной работы (КСР) – 35 час.

Вид учебной работы	Всего	Семестр
--------------------	-------	---------

	часов	2
<b>ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ</b>	216	216
КОНТАКТНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ С ПРЕПОДАВАТЕЛЕМ, в том числе:	69	69
Лекции (Лек)	32	32
Практические (семинарские) занятия (Пр)	32	32
Контроль самостоятельной работы и иная контактная работа (КСР)	2	2
Консультации (Конс)	2	2
Контактные часы во время аттестации (КПА)	1	1
САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ (СРС), в том числе:	112	112
Подготовка к промежуточной аттестации в форме: (экзамен)	35	35
ФОРМА ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ (За – зачет, ЗО – зачет с оценкой, Э – экзамен)	Эк	Эк

### 3.2. Содержание дисциплины, структурированное по разделам и видам занятий

Разделы дисциплины	Семестр	Распределение трудоемкости (в часах) по видам учебной работы, включая СРС									Формируемые результаты обучения (знания, умения, навыки)	Литература	Формы текущего контроля успеваемости	Формы промежуточной аттестации	Максимальное количество баллов по балльно - рейтинговой системе
		Занятия лекционного типа	Занятия практического / семинарского типа	Лабораторные работы	Групповые консультации	Самостоятельная работа студента, в том числе контроль самостоятельной работы	подготовка (зачет) к промежуточной аттестации	Сдача зачета / экзамена	Итого						
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Раздел 1. Корпоративные информационные системы как объект защиты от	2	4	4	-	-	14				22	ПК 2.1, ПК 2.2	Л1. 1, Л2. 1	Тест		6

угроз ИБ.																	
Раздел 2. Моделирова ние угроз безопасност и информации	2	4	4	-	-	1 4				2 2	ПК 2.1, ПК 2.2	Л1. 1, Л1. 2	Тест				6
Раздел 3. Управление информацион ной безопасность ю	2	4	4	-	-	1 4				2 2	ПК 2.1, ПК 2.2	Л1. 1, Л1. 2	Тест				6
Раздел 4. Международ ные стандарты в сфере управления рисками ИБ	2	4	4	-	-	1 4	2			2 2	ПК 2.1, ПК 2.2	Л1. 1, Л1. 2	Тест				6
Раздел 5. Современны е методики оценки рисков ИБ	2	4	4	-	-	1 4				2 2	ПК 2.1, ПК 2.2		Тест				6
Раздел 6. Этапы оценки рисков ИБ	2	4	4	-	-	1 4				2 2	ПК 2.1, ПК 2.2		Тест				10
Раздел 7. Обработка рисков ИБ	2	4	4	-	-	1 4				2 2	ПК 2.1, ПК 2.2		Тест				10
Раздел 8. Меры обеспечения ИБ	2	4	4	-	-	1 4				2 2	ПК 2.1, ПК 2.2		Тест				10
Промежуточ ная аттестация	2				2		2	3 5	1	4 0	ПК 2.1, ПК 2.2	Л1. 1, Л1. 2		Э			40
<b>Итого</b>	2	<b>3 2</b>	<b>32</b>		<b>2</b>	<b>1 1 2</b>	<b>2</b>		<b>1</b>	<b>216</b>							<b>100</b>

### 3.3. Тематический план лекционных занятий

№ п/п	Темы лекционных занятий	Трудоемкость, час.
1	Архитектура корпоративных информационных систем. Угрозы, уязвимости и риски ИБ корпоративных информационных систем.	2

2	Моделирование угроз безопасности информации. Методики оценки угроз ИБ (Методика ФСТЭК России, методика на базе подходов и инструментов MITRE). Формирование сценариев атак на информационные ресурсы корпоративных информационных систем.	4
3	Принципы управления информационной безопасностью. Управление рисками ИБ. Терминология управления рисками. Цель процесса оценки рисков. Оценка рисков и базовый уровень защиты. Количественный и качественный анализ рисков	6
4	Международные стандарты в сфере управления рисками ИБ (NIST SP800-30, ISO27005)	4
5	Современные методики оценки рисков ИБ (CRAMM, Octave, Microsoft)	4
6	Основные этапы анализа рисков ИБ. Идентификация активов. Оценка ценности активов. Идентификация угроз и уязвимостей. Оценка вероятности реализации угроз. Вычисление уровня риска. Выбор шкалы уровня риска и приемлемого уровня риска	4
7	Обработка рисков. Избежание риска. Перенос риска. Меры противодействия и остаточный уровень риска. Обоснованное принятие риска. Роли и ответственность в процессе управления рисками. Владельцы активов корпоративных информационных систем.	4
8	Меры обеспечения ИБ. Системы обеспечения информационной безопасности (СОИБ). Формирование требований к СОИБ корпоративных информационных систем на базе результатов оценки рисков и угроз ИБ. Нормативные требования к СОИБ.	4
<b>Всего</b>		<b>32</b>

### 3.4. Тематический план практических занятий

№ п/п	Темы практических занятий	Трудоемкость, час.
1	Инструментальный анализ защищенности виртуальной информационной инфраструктуры. Применение сканеров сетевой безопасности и формирование отчета об уязвимостях инфраструктуры.	4
2	Разработка модели угроз ИБ для корпоративной информационной системы с использованием матрицы техник нарушителей MITRE ATT&CK и построением Cyber Kill Chain	4
3	Разработка модели угроз ИБ для корпоративной информационной системы на базе методических документов ФСТЭК и БДУ ФСТЭК	4
4	Изучение методик оценки рисков ИБ и их сравнительный анализ	4
5	Оценка рисков ИБ для примера корпоративной информационной системы на основе ГОСТ Р ИСО/МЭК 27005-2010	4
6	Разработка политики информационной безопасности предприятия.	4
7	Изучение групп мер обеспечения ИБ согласно приказам ФСТЭК №21 (ИСПДн), 239 (КИИ)	4
8	Разработка технического задания на СОИБ согласно нормативным требованиям и результатам анализа рисков ИБ	4



### 3.5. Тематический план лабораторных работ

Данный вид работы не предусмотрен учебным планом.

### 3.6. Самостоятельная работа студента

Номер раздела дисциплины	Вид СРС	Содержание СРС	Трудовая емкость, час
1	Изучение теоретического материала, подготовка к практическому занятию	Изучение документации на инструментальные средства анализа защищенности nmap, Metasploit Framework, OpenVAS, сканера уязвимостей ScanOVAL.	14
2	Изучение теоретического материала, подготовка к практическому занятию	Изучение матрицы техник нарушителей MITRE ATT&CK, документации к матрице. Изучение концепции построения Cyber Kill Chain	14
3	Изучение теоретического материала, подготовка к практическому занятию	Изучение методики оценки угроз безопасности информации ФСТЭК от 05.02.2021 г., матрицы техник нарушителей.	14
4	Изучение теоретического материала, подготовка к практическому занятию	Изучение методик оценки рисков ИБ: CRAMM, Octave, Microsoft, COBIT, NIST SP800	14
5	Изучение теоретического материала, подготовка к практическому занятию	Изучение стандарта ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.	14
6	Изучение теоретического материала, подготовка к практическому занятию	Политика информационной безопасности предприятия. Назначение и состав документа.	14
7	Изучение теоретического материала, подготовка к практическому занятию	Меры обеспечения ИБ. Организационные меры обеспечения ИБ. Технические меры обеспечения ИБ. Приказ ФСТЭК от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Приказ ФСТЭК России от 25.12.2017 N 239 (ред. от 20.02.2020) "Об утверждении	14

		Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации"	
8	Изучение теоретического материала, подготовка к практическому занятию	Рискориентированный подход к обеспечению ИБ корпоративных информационных систем. Приказ ФСТЭК России от 21.12.2017 N 235 (ред. от 20.04.2023) "Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования".	14

#### 4. Образовательные технологии

При проведении учебных занятий используются традиционные образовательные технологии (лекции в сочетании с практическими занятиями, семинарами, самостоятельное изучение определённых разделов) и современные образовательные технологии, направленные на обеспечение развития у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств: интерактивные лекции, групповые дискуссии, деловые игры, проблемное обучение, тренинги, работа в команде, case-study.

При реализации дисциплины «Информационная безопасность в корпоративных информационных системах» по образовательной программе направления подготовки бакалавриата 09.04.03 «Прикладная информатика» применяются электронные образовательные технологии.

В процессе обучения используются электронные образовательные ресурсы (ЭОР), размещенные в личных кабинетах обучающихся Электронного университета КГЭУ, URL: <http://e.kgeu.ru/>; на площадке LMS Moodle.

#### 5. Оценка результатов обучения

Оценивание результатов обучения по дисциплине осуществляется в рамках текущего контроля успеваемости, проводимого по балльно-рейтинговой системе (БРС), и промежуточной аттестации.

Текущий контроль успеваемости осуществляется в течение семестра, включает: индивидуальный или групповой опрос, контрольные работы, защиты рефератов, защиты презентаций проектов, др. заданий, выполненных индивидуально или группой обучающихся.

Итоговой оценкой результатов освоения дисциплины является оценка, выставленная во время промежуточной аттестации обучающегося (экзамен) с учетом результатов текущего контроля успеваемости.

На экзамен выносятся теоретические и практические задания, проработанные в течение семестра на учебных занятиях и в процессе самостоятельной работы обучающихся.

Обобщенные критерии и шкала оценивания уровня сформированности компетенции (индикатора достижения компетенции) по итогам освоения дисциплины:

Планируемые результаты обучения	Обобщенные критерии и шкала оценивания результатов обучения			
	неудовлетворительно	удовлетворительно	хорошо	отлично
	не зачтено	зачтено		
Полнота знаний	Уровень знаний ниже минимальных требований, имеют место грубые ошибки	Минимально допустимый уровень знаний, имеет место много негрубых ошибок	Уровень знаний в объеме, соответствующем программе, имеет место несколько негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок
Наличие умений	При решении стандартных задач не продемонстрированы основные умения, имеют место грубые ошибки	Продемонстрированы основные умения, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объеме	Продемонстрированы все основные умения, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объеме, но некоторые с недочетами	Продемонстрированы все основные умения, решены все основные задачи с отдельными несущественными недочетами, выполнены все задания в полном объеме
Наличие навыков (владение опытом)	При решении стандартных задач не продемонстрированы базовые навыки, имеют место грубые ошибки	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов
Характеристика сформированности компетенции (индикатора достижения компетенции)	Компетенция в полной мере не сформирована. Имеющихся знаний, умений, навыков недостаточно для решения практических (профессиональных) задач	Сформированность компетенции соответствует минимальным требованиям. Имеющихся знаний, умений, навыков в целом достаточно для решения практических (профессиональных) задач, но требуется дополнительная практика по большинству практических задач	Сформированность компетенции в целом соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в целом достаточно для решения стандартных практических (профессиональных) задач	Сформированность компетенции полностью соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в полной мере достаточно для решения сложных практических (профессиональных) задач

Уровень сформированности компетенции (индикатора достижения компетенции)	Низкий	Ниже среднего	Средний	Высокий

Шкала оценки результатов обучения по дисциплине:

Код компетенции	Код индикатора достижения компетенции	Запланированные результаты обучения по дисциплине	Уровень сформированности компетенции (индикатора достижения компетенции)			
			Высокий	Средний	Ниже среднего	Низкий
			Шкала оценивания			
			отлично	хорошо	удовлетворительно	неудовлетворительно
			зачтено		не зачтено	
ПК-2	ПК-2.1	<i>Знать:</i>				
		Архитектуру информационных систем предприятий и организаций (31)	Свободно и в полном объеме описывает современную архитектуру информационных систем для решения профессиональных задач.	Достаточно полно знает современную архитектуру информационных систем для решения профессиональных задач, допускает незначительное количество ошибок.	Плохо описывает современную архитектуру информационных систем для решения профессиональных задач, допускает много ошибок.	Не знает современную архитектуру информационных систем для решения профессиональных задач.
		<i>Уметь:</i>				
		Выбирать методологию и технологию проектирования информационных систем (У1)	Свободно выбирает технологию проектирования информационных систем для решения профессиональных задач.	Умеет использовать технологию проектирования информационных систем для решения профессиональных задач, допускает незначительные ошибки.	Слабо ориентируется в технологии проектирования информационных систем для решения профессиональных задач.	Не умеет использовать технологию проектирования информационных систем для решения профессиональных задач.
<i>Владеть:</i>						
Методами построения различных типов	Демонстрирует навыки построения	Демонстрирует базовые навыки	Имеет минимальный набор навыков	Не демонстрирует навыки		

		информационных систем (В1)	различных типов информационных систем для решения профессиональных задач.	построения различных типов информационных систем для решения профессиональных задач. Допущен ряд незначительных ошибок.	навыки построения различных типов информационных систем для решения профессиональных задач.	построения различных типов информационных систем для решения профессиональных задач.
ПК-2	ПК-2.2	<i>Знать:</i>				
		Современные методы и инструментальные средства прикладной информатики для автоматизации и решения профессиональных задач (З1)	Свободно и в полном объеме описывает современные методы и инструментальные средства прикладной информатики для автоматизации и решения профессиональных задач.	Достаточно полно знает современные методы и инструментальные средства прикладной информатики для автоматизации и решения профессиональных задач.	Плохо описывает современные методы и инструментальные средства прикладной информатики для автоматизации и решения профессиональных задач.	Не знает современные методы и инструментальные средства прикладной информатики для автоматизации и решения профессиональных задач.
		<i>Уметь:</i>				
		Обосновывать выбор современных методов и инструментальных средств прикладной информатики для автоматизации и решения профессиональных задач (У1)	Свободно обосновывает выбор современных методов и инструментальных средств прикладной информатики для автоматизации и решения профессиональных задач.	Обосновывает выбор современных методов и инструментальных средств прикладной информатики для автоматизации и решения профессиональных задач, допуская незначительные ошибки.	Слабо ориентируется в современных методах и инструментальных средствах прикладной информатики для автоматизации и решения профессиональных задач.	Не умеет обосновывать выбор современных методов и инструментальных средств прикладной информатики для автоматизации и решения профессиональных задач.
<i>Владеть:</i>						
		Навыками применения современных методов и инструментальных средств прикладной информатики для автоматизации и решения	Свободно владеет навыками применения современных методов и инструментальных средств прикладной информатики для	Демонстрирует базовые навыки применения современных методов и инструментальных средств прикладной информатики	Имеет минимальный набор навыков применения современных методов и инструментальных средств прикладной информатики для	Не демонстрирует базовые навыки применения современных методов и инструментальных средств прикладной информатики

		профессиональ- ных задач (B1)	автоматизации и решения профессиональ ных задач.	для автоматиза- ции и решения профессиона льных задач.	автоматизации и решения профессиональ ных задач.	для автоматизации и решения профессиональ ных задач.
--	--	----------------------------------	---	---	---	--

Оценочные материалы для проведения текущего контроля успеваемости и промежуточной аттестации приведены в Приложении к рабочей программе дисциплины. Полный комплект заданий и материалов, необходимых для оценивания результатов обучения по дисциплине, хранится на кафедре-разработчике в бумажном и электронном виде.

## **5. Учебно-методическое и информационное обеспечение дисциплины**

### **5.1. Учебно-методическое обеспечение**

#### **5.1.1 Основная литература**

1. Капгер, И. В. Управление информационной безопасностью : учебное пособие / И. В. Капгер, А. С. Шабуров. — Пермь : ПНИПУ, 2023. — 91 с. — ISBN 978-5-398-02866-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/328889> (дата обращения: 20.04.2023). — Режим доступа: для авториз. пользователей.

2. Нестеров, С. А. Основы информационной безопасности / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2023. — 324 с. — ISBN 978-5-507-48149-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/341267> (дата обращения: 20.04.2023). — Режим доступа: для авториз. пользователей.

#### **5.1.2 Дополнительная литература**

1. Николаев, Н. С., Управление информационной безопасностью : учебник / Н. С. Николаев. — Москва : КноРус, 2021. — 188 с. — ISBN 978-5-406-07325-4. — URL: <https://book.ru/book/939841> (дата обращения: 20.04.2023). — Текст : электронный.

2. Проектирование, разработка и обеспечение безопасности информационных систем : монография / В. В. Бабенко, Р. А. Гашин, Ю. В. Гольчевский [и др.]. — Сыктывкар : СГУ им. Питирима Сорокина, 2016. — 146 с. — ISBN 978-5-87661-395-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/176919> (дата обращения: 20.04.2023). — Режим доступа: для авториз. пользователей.

3. Коваленко, Ю. И., Методика защиты информации в организациях : монография / Ю. И. Коваленко, Г. И. Москвитин, М. М. Тараскин. — Москва : Русайнс, 2020. — 162 с. — ISBN 978-5-4365-0887-0. — URL: <https://book.ru/book/934719> (дата обращения: 20.04.2023). — Текст : электронный.

## 6.2. Информационное обеспечение

### 6.2.1. Электронные и интернет-ресурсы

№ п/п	Наименование электронных и интернет-ресурсов	Ссылка
1	Электронно-библиотечная система «Лань»	<a href="https://e.lanbook.com/">https://e.lanbook.com/</a>
2	Электронно-библиотечная система «ibooks.ru»	<a href="https://ibooks.ru/">https://ibooks.ru/</a>
3	Электронно-библиотечная система «book.ru»	<a href="https://www.book.ru/">https://www.book.ru/</a>
4	Энциклопедии, словари, справочники	<a href="http://www.rubricon.com">http://www.rubricon.com</a>
5	Портал "Открытое образование"	<a href="http://npoed.ru">http://npoed.ru</a>
6	Единое окно доступа к образовательным ресурсам	<a href="http://window.edu.ru">http://window.edu.ru</a>
7	MITRE ATT&CK	<a href="https://attack.mitre.org/">https://attack.mitre.org/</a>

### 6.2.2. Профессиональные базы данных

№ п/п	Наименование профессиональных баз данных	Адрес	Режим доступа
1	Официальный интернет-портал правовой информации	<a href="http://pravo.gov.ru">http://pravo.gov.ru</a>	
2	Справочная правовая система «Консультант Плюс»	<a href="http://consultant.ru">http://consultant.ru</a>	
3	Справочно-правовая система по законодательству РФ	<a href="http://garant.ru">http://garant.ru</a>	

### 6.2.3. Информационно-справочные системы

№ п/п	Наименование информационно-справочных систем	Адрес	Режим доступа
1	Научная электронная библиотека	<a href="http://elibrary.ru">http://elibrary.ru</a>	
2	Российская государственная библиотека	<a href="http://www.rsl.ru">http://www.rsl.ru</a>	
3	Международная реферативная база данных научных изданий zbMATH	<a href="http://www.zbmath.org">http://www.zbmath.org</a>	
4	Международная реферативная база данных научных изданий Springerlink	<a href="http://link.springer.com">http://link.springer.com</a>	
5	Образовательный портал	<a href="http://www.uceba.com">http://www.uceba.com</a>	

### 6.2.4. Лицензионное и свободно распространяемое программное обеспечение дисциплины

№ п/п	Наименование программного обеспечения	Способ распространения (лицензионное/свободно)	Реквизиты подтверждающих документов
2	Браузер Chrome	Система поиска информации в сети интернет	Свободная лицензия Неискл. право. Бессрочно
3	LMS Moodle	ПО для эффективного онлайн-взаимодействия преподавателя и студента	Свободная лицензия Неискл. право. Бессрочно

## 7. Материально-техническое обеспечение дисциплины



№ п/п	Вид учебной работы	Наименование специальных помещений и помещений для СРС	Оснащенность специальных помещений и помещений для СРС
1	Лекционные занятия	Учебная аудитория для проведения занятий лекционного типа	персональный компьютер (26 шт.), интерактивная доска, мультимедийный проектор.
2	Практические занятия	Учебная аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	персональный компьютер (26 шт.), интерактивная доска, мультимедийный проектор.
3	Самостоятельная работа обучающегося	Компьютерный класс с выходом в Интернет В-600а	Специализированная учебная мебель на 30 посадочных мест, 30 компьютеров, технические средства обучения (мультимедийный проектор, компьютер (ноутбук), экран), видеокамеры, программное обеспечение
		Читальный зал библиотеки	Специализированная мебель, компьютерная техника с возможностью выхода в Интернет и обеспечением доступа в ЭИОС, мультимедийный проектор, экран, программное обеспечение

## 8. Особенности организации образовательной деятельности для лиц с ограниченными возможностями здоровья и инвалидов

Лица с ограниченными возможностями здоровья (ОВЗ) и инвалиды имеют возможность беспрепятственно перемещаться из одного учебно-лабораторного корпуса в другой, подняться на все этажи учебно-лабораторных корпусов, заниматься в учебных и иных помещениях с учетом особенностей психофизического развития и состояния здоровья.

Для обучения лиц с ОВЗ и инвалидов, имеющих нарушения опорно-двигательного аппарата, обеспечены условия беспрепятственного доступа во все учебные помещения. Информация о специальных условиях, созданных для обучающихся с ОВЗ и инвалидов, размещена на сайте университета [www/kgeu.ru](http://www/kgeu.ru). Имеется возможность оказания технической помощи ассистентом, а также услуг сурдопереводчиков и тифлосурдопереводчиков.

Для адаптации к восприятию лицами с ОВЗ и инвалидами с нарушенным слухом справочного, учебного материала по дисциплине обеспечиваются следующие условия:

- для лучшей ориентации в аудитории, применяются сигналы оповещения о начале и конце занятия (слово «звонок» пишется на доске);
- внимание слабослышащего обучающегося привлекается педагогом жестом (на плечо кладется рука, осуществляется нерезкое похлопывание);
- разговаривая с обучающимся, педагогический работник смотрит на него, говорит ясно, короткими предложениями, обеспечивая возможность чтения по губам.

Компенсация затруднений речевого и интеллектуального развития слабослышащих обучающихся проводится путем:

- использования схем, диаграмм, рисунков, компьютерных презентаций с гиперссылками, комментирующими отдельные компоненты изображения;
- регулярного применения упражнений на графическое выделение существенных признаков предметов и явлений;
- обеспечения возможности для обучающегося получить адресную консультацию по электронной почте по мере необходимости.

Для адаптации к восприятию лицами с ОВЗ и инвалидами с нарушениями зрения справочного, учебного, просветительского материала, предусмотренного образовательной программой по выбранному направлению подготовки, обеспечиваются следующие условия:

- ведется адаптация официального сайта в сети Интернет с учетом особых потребностей инвалидов по зрению, обеспечивается наличие крупношрифтовой справочной информации о расписании учебных занятий;
- педагогический работник, его собеседник (при необходимости), присутствующие на занятии, представляются обучающимся, при этом каждый раз называется тот, к кому педагогический работник обращается;
- действия, жесты, перемещения педагогического работника коротко и ясно комментируются;
- печатная информация предоставляется крупным шрифтом (от 18 пунктов), тотально озвучивается;
- обеспечивается необходимый уровень освещенности помещений;
- предоставляется возможность использовать компьютеры во время занятий и право записи объяснений на диктофон (по желанию обучающихся).

Форма проведения текущей и промежуточной аттестации для обучающихся с ОВЗ и инвалидов определяется педагогическим работником в соответствии с учебным планом. При необходимости обучающемуся с ОВЗ, инвалиду с учетом их индивидуальных психофизических особенностей дается возможность пройти промежуточную аттестацию устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п., либо предоставляется дополнительное время для подготовки ответа.

## Лист внесения изменений

Дополнения и изменения в рабочей программе дисциплины на 20\_\_\_\_  
/20\_\_\_\_ учебный год

В программу вносятся следующие изменения:

1. \_\_\_\_\_
2. \_\_\_\_\_
3. \_\_\_\_\_

*Указываются номера страниц, на которых внесены изменения,  
и кратко дается характеристика этих изменений*

Программа одобрена на заседании кафедры –разработчика «\_\_\_\_» \_\_\_\_\_  
20\_г., протокол № \_\_\_\_\_

Зав. кафедрой \_\_\_\_\_ И.О. Фамилия  
Подпись, дата

Программа одобрена методическим советом института \_\_\_\_\_  
«\_\_\_\_» \_\_\_\_\_ 20\_\_\_\_ г., протокол № \_\_\_\_\_

Зам. директора по УМР \_\_\_\_\_ И.О. Фамилия  
Подпись, дата

Согласовано:

Руководитель ОПОП \_\_\_\_\_ И.О. Фамилия  
Подпись, дата

*Приложение к  
рабочей  
программе дисциплины*



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
Федеральное государственное бюджетное образовательное  
учреждение высшего образования  
«КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭНЕРГЕТИЧЕСКИЙ УНИВЕРСИТЕТ»  
(ФГБОУ ВО «КГЭУ»)

## **ОЦЕНОЧНЫЕ МАТЕРИАЛЫ**

**по дисциплине**

**Б1.В.ДЭ.01.01.01 Информационная безопасность в корпоративных  
информационных системах**

---

Направление  
подготовки

09.04.03 Прикладная информатика

Направленность (профиль) Интеллектуальные и информационные системы  
предприятий и организаций

Квалификация

Магистр

г. Казань, 2023

Оценочные материалы по дисциплине «Информационная безопасность в корпоративных информационных системах» - комплект контрольно-измерительных материалов, предназначенных для оценивания результатов обучения на соответствие индикаторам достижения компетенции:

ПК-2.1 Проектирует архитектуру ИС предприятий и организаций в прикладной области с учетом требований заказчика

ПК-2.2 Применяет современные методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания ИС

Текущий контроль успеваемости обеспечивает оценивание процесса обучения по дисциплине. При текущем контроле успеваемости используются следующие оценочные средства: защита практических работ; презентаций рефератов, тестирование с использованием компьютера. Промежуточная аттестация имеет целью определить уровень достижения запланированных результатов обучения по дисциплине за 1 курс 2 семестра. Форма промежуточной аттестации – экзамен.

Оценочные материалы включают задания для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся, разработанные в соответствии с рабочей программой дисциплины.

### 1. Технологическая карта

#### Семестр \_2

Номер раздела/ темы дис- циплины	Вид СРС	Наимено- вание оценочного средства	Заплани- рованные дескрипторы освоения дисциплины	Уровень освоения дисциплины, баллы			
				неудов-но	удов-но	хорошо	отлично
				не зачтено	зачтено		
				низкий	ниже среднего	средний	высокий
Текущий контроль успеваемости							
1	Изучение теоретического материала, подготовка к практическому занятию	Отчет по практической работе	ПК- 2.1 ПК- 2.2	<2	2-3	4-5	6-7
2	Изучение теоретического материала, подготовка к практическому занятию	Отчет по практической работе	ПК- 2.1 ПК- 2.2	<2	2-3	4-5	6-7
3	Изучение теоретичес	Отчет по практическ	ПК- 2.1 ПК- 2.2	<2	2-3	4-5	6-7

	ского материала, подготовка к практическому занятию	ой работе					
4	Изучение теоретического материала, подготовка к практическому занятию	Отчет по практической работе	ПК- 2.1 ПК- 2.2	<2	2-3	4-5	6-7
5	Изучение теоретического материала, подготовка к практическому занятию	Отчет по практической работе	ПК- 2.1 ПК- 2.2	<4	4-5	5-6	7-8
6	Изучение теоретического материала, подготовка к практическому занятию	Отчет по практической работе	ПК- 2.1 ПК- 2.2	<4	4-5	5-6	7-8
7	Изучение теоретического материала, подготовка к практическому занятию	Отчет по практической работе	ПК- 2.1 ПК- 2.2	<4	4-5	5-6	7-8
8	Изучение теоретического материала, подготовка к практическому занятию	Отчет по практической работе	ПК- 2.1 ПК- 2.2	<4	4-5	5-6	7-8

Всего баллов				менее 28	28-44	44-52	52-60
Промежуточная аттестация							
Подготовка к экзамену	Задания к экзамену	ПК- 2.1 ПК- 2.2	менее 19	20-25	26-32	33-40	
<b>Итого баллов</b>				<b>0-47</b>	<b>48-69</b>	<b>70-84</b>	<b>85-100</b>

## 2. Перечень оценочных средств

Краткая характеристика оценочных средств, используемых при текущем контроле успеваемости и промежуточной аттестации обучающегося по дисциплине:

Наименование оценочного средства	Краткая характеристика оценочного средства	Оценочные материалы
Отчет по практической работе (От)	Письменная работа (в электронном виде), выполненная согласно выданному заданию	Комплект методических указаний к выполнению практических работ
Экзамен (Э)	Средство контроля усвоения учебного материала разделов дисциплины, организованное в виде письменной работы и последующего собеседования преподавателя с обучающимся	Экзаменационные билеты по темам/разделам дисциплины

## 3. Оценочные материалы текущего контроля успеваемости обучающихся

Наименование оценочного средства	Отчет по практической работе (От)
	Письменная работа (в электронном виде), выполненная согласно выданному заданию.  Перечень практических работ представлен в разделе 3.4.
Критерии оценки и шкала оценивания в баллах	Критерии оценки: 1) Соответствие содержания выполненной работы заданию. 2) Полнота выполненных заданий 3) Корректность оформления 4) Своевременность

## 4. Оценочные материалы промежуточной аттестации

Наименование оценочного средства	Экзамен
----------------------------------	---------

<p>Представление и содержание оценочных материалов</p>	<p>Оценочные материалы, вынесенные на экзамен, состоят из экзаменационных билетов. Билет содержит два вопроса по теоретическому материалу и задание практического характера для проверки практических умений. Всего 25 экзаменационных билетов.</p> <p>Примеры вопросов к экзамену:</p> <ol style="list-style-type: none"> <li>1. Классификация угроз ИБ корпоративных информационных систем</li> <li>2. Классификация уязвимостей ИБ корпоративных информационных систем. Оценка уровня критичности уязвимости согласно CVSS 3.0.</li> <li>3. Цели и задачи моделирования угроз безопасности информации.</li> <li>4. Основные этапы моделирования угроз безопасности информации согласно методике ФСТЭК.</li> <li>5. Принципы формирования сценариев атак на информационные ресурсы корпоративных информационных систем.</li> <li>6. Матрица тактик и техник нарушителей MITRE ATT&amp;CK. Виды матриц Enterprise, ICS, Mobile. Способы применения матрицы.</li> <li>7. Принципы управления информационной безопасностью.</li> <li>8. Управление рисками ИБ. Основные понятия управления рисками.</li> <li>9. Цель процесса оценки рисков. Оценка рисков и базовый уровень защиты.</li> <li>10. Количественный и качественный анализ рисков ИБ</li> <li>11. Стандарт в сфере управления рисками ИБ NIST SP800-30</li> <li>12. Методика оценки рисков ИБ CRAMM</li> <li>13. Методика оценки рисков ИБ Octave</li> <li>14. Методика оценки рисков ИБ FRAP</li> <li>15. Методика оценки рисков ИБ RiskWatch</li> <li>16. Методика оценки рисков ИБ Microsoft</li> <li>17. Основные этапы анализа рисков ИБ. Идентификация активов.</li> <li>18. Основные этапы анализа рисков ИБ. Оценка ценности активов.</li> <li>19. Основные этапы анализа рисков ИБ. Идентификация угроз и уязвимостей.</li> <li>20. Основные этапы анализа рисков ИБ. Оценка вероятности реализации угроз. Вычисление уровня риска.</li> <li>21. Выбор шкалы уровня риска и приемлемого уровня риска</li> <li>22. Обработка рисков. Избежание риска. Перенос риска.</li> <li>23. Меры противодействия и остаточный уровень риска. Обоснованное принятие риска.</li> <li>24. Роли и ответственность в процессе. управления рисками. Владельцы активов корпоративных информационных систем.</li> <li>25. Меры обеспечения ИБ. Системы обеспечения информационной безопасности (СОИБ).</li> <li>26. Формирование требований к СОИБ корпоративных информационных систем на базе результатов оценки рисков и угроз ИБ.</li> <li>27. Нормативные требования к СОИБ.</li> </ol>
<p>Критерии оценки и шкала оценивания в баллах</p>	<p>Число баллов, которое может получить обучающийся за экзамен, составляет от 20 до 40.</p> <p>При выставлении баллов за ответы на вопросы и задание в билете учитываются следующие критерии:</p> <p>При выставлении баллов за ответы на вопросы учитываются следующие критерии:</p> <ol style="list-style-type: none"> <li>1. Знание понятий, категорий</li> <li>2. Владение методами и технологиями, запланированными в РПД</li> <li>3. Владение специальными терминами и использование их при ответе.</li> <li>4. Умение объяснять, делать выводы и обобщения, давать аргументированные ответы</li> <li>5. Логичность и последовательность ответа</li> </ol> <p>Ответ показывает прочные знания основных процессов изучаемой предметной</p>



	<p>области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа – <b>29-32</b> баллов.</p> <p>Ответ показывает прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа. Однако допускаются одна – две неточности в ответе – <b>24-28</b> балла.</p> <p>Ответ не полный, с недостаточной глубиной и полнотой раскрытия – <b>20-23</b> баллов.</p> <p>При выставлении баллов за задание в билете учитываются правильность выполнения практического задания</p> <p>Задание выполнено полностью – <b>8</b> балла</p> <p>Задание выполнено с ошибками – <b>4-7</b> балла</p> <p>Много ошибок – <b>1-3</b></p> <p>Не выполнено – <b>0</b> баллов</p> <p><b>Максимальное количество баллов за экзамен – 40 баллов</b></p>
--	--