Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

Троицкий Александр Витальевич

Подписано цифровой подписью: Троицкий Александр Витальевич

«УТВЕРЖДАЮ»
И.о. проректора
_____ А.В. Троицкий
«___»_____2023 г.

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.ДВ.01.01 «ЭКОНОМИКО-УПРАВЛЕНЧЕСКИЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки: 10.04.01 - Информационная безопасность
Направленность (профиль): Менеджмент информационной безопасности
Уровень высшего образования: Магистратура
Форма обучения: очная

Королев
2023

Рабочая программа является составной частью основной профессиональной образовательной программы и проходит рецензирование со стороны работодателей в составе основной профессиональной образовательной программы. Рабочая программа актуализируется и корректируется ежегодно.

Автор: Смирнова П.В. Рабочая программа дисциплины (модуля): Экономико-управленческие аспекты обеспечения информационной безопасности . – Королев МО: «Технологический Университет», 2023

Рецензент: Сухотерин А.И.

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по 10.04.01 направление подготовки -Информационная безопасность и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 11.04.2023 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	Соляной В.Н к.в.н. доцент			
Год утверждения (переутверждения)	2023	2024		
Номер и дата протокола заседания кафедры	№8 от 29.03.2023г.			

Рабочая программа согласована:
Руководитель ОПОП ВО Сухотерин А.И.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2023	2024		
Номер и дата протокола заседания УМС	№5 от 11.04.2023г.			

2

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОПОП

Целью изучения дисциплины является: формирование у обучаемых концептуальных и методологических подходов в области экономико-управленческих основ обеспечения информационной безопасности региона в процессе развития современного информационного общества.

В процессе обучения по направлению подготовки 10.04.01 «Информационная безопасность», студент приобретает и совершенствует следующие компетенции:

Универсальные компетенции:

- УК-1: Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.

Профессиональные компетенции:

- ПК-2: Способен разрабатывать проектные решения по развитию автоматизированных ИАС в защищенном исполнении.

Основными **задачами** дисциплины являются:

1. раскрытие сущности, целей и содержание экономико-управленческих основ обеспечения информационной безопасности региона;
2. освоение содержания базовых экономико-управленческих компонентов обеспечения информационной безопасности;
3. раскрытие сущности и содержания экономико-управленческих принципов обеспечения информационной безопасности региона;
4. овладение методологическими основами экономико-управленческих процессов обеспечения информационной безопасности региона;
5. освоение методологии и организации процесса разработки экономико-управленческих решений в области обеспечения информационной безопасности;
6. овладение методиками определения информационных рисков при реализации выработанных управленческих решений в области информационной безопасности региона;
7. определение методологических подходов комплексной функциональной и экономической оценки эффективности принимаемых управленческих решений по обеспечению информационной безопасности;
8. овладение методологией управления информационными рисками критериями и методами оценки эффективности проектов по обеспечению информационной безопасности;
9. определение общих методологических подходов построения систем управления информационной безопасностью информационных объектов региона.

Показатель освоения компетенции отражают следующие индикаторы:

Трудовые действия:

- УК-1.3 Использует методы системного и критического анализа, анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними.
- ПК-2.3. Разрабатывать проекты документов по созданию защищенных технологий с оформлением технических заданий на проектирование, осуществлять непосредственную разработку проектных решений по ИБ и оценку их эффективности в автоматизированной ИАС.

Необходимые умения:

- УК-1.2. Определяет уязвимости и угрозы информационной безопасности, необходимые для выявления и решения проблемной ситуации, планирует мероприятия и процессы по их устранению на основе системного и междисциплинарных подходов.
- ПК-2.2. Проводить предпроектное обследование с выбором перспективной технологии защиты автоматизированной ИАД с разработкой проектной документации и комплексной оценкой эффективности применения автоматизированной ИАС.

Необходимые знания:

- ПК-2.1. Знать нормативную базу создания и эксплуатации защищенных функциональных и обеспечивающих подсистем, методы проектирования, критерии и показатели эффективности автоматизированной ИАС.
- УК-1.1. Ставит цель, определяет способы ее достижения, разрабатывает стратегию действия, принимает конкретные решения для ее реализации с учетом требований регуляторов в области защиты информации.

2. Место дисциплины (модуля) в структуре ОПОП ВО.

Дисциплина «Экономико-управленческие аспекты, обеспечения информационной безопасности» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений, основной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность», профиль подготовки – Менеджмент информационной безопасности региона.

Дисциплина базируется на ранее изученных дисциплинах: “Специальные разделы математики»; «Теоретические основы управления»; «Защищенные информационные системы»; «Экономика и управление» и компетенциях: УК-1, 2; ПК-2; ОПК-1.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми при выполнении выпускной диссертационной работы магистра.

3.Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 6 зачетных единиц, 216 часа.

Таблица 1

Виды занятий	Всего часов	Семестр 3	Семестр …	Семестр …	Семестр …
Общая трудоемкость	**216**	**216**			
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	**46**	**46**			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	24	24			
Лабораторные работы (ЛР)					
Другие виды контактной работы	**6**	**6**			
Практическая подготовка					
Самостоятельная работа	**168**	**168**			
Курсовые работы (проекты) *					
*Расчетно-графические работы**					
*Контрольная работа, домашнее задание**	+	+			
Текущий контроль знаний *	**Тест**	**Тест**			
Вид итогового контроля	**Экзамен**	**Экзамен**			

* Под другими видами контактной работы понимается: групповые и индивидуальные консультации, тестирование.

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1.Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час.	Практ. занятия, час.	Занятия в интерактивной форме, час	Код компетенций
Раздел (модуль) 1. Организационно-экономические аспекты обеспечения информационной безопасности (РАЗВИТИЕ СИСТЕМЫ ЭКОНОМИКО-ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ РЕГИОНА НА БАЗЕ КОРПОРАТИВНЫХ МЕХАНИЗМОВ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ)				
Тема 1. Введение в дисциплину и существующие подходы организационно-экономического обеспечения информационной безопасности региона	4	6	3	УК-1 ПК-2.
Тема 2. Основные положения новых подходов организационно-экономического обеспечения информационной безопасности региона	4	6	2	УК-1 ПК-2
Раздел (модуль) 2. Организационно-управленческие аспекты обеспечения информационной безопасности (ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПРИНЯТИИ ОРГАНИЗАЦИОННО-УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ)				
Тема 3. Существующие основы обеспечения информационной безопасности принятии региональных организационно-управленческих решений	4	6	4	УК-1 ПК-2
Тема 4. Основные положения новых подходов по обеспечения информационной безопасности принятии региональных организационно-управленческих решений	4	6	3	УК-1 ПК-2.
Итого:	**16**	**24**	**12**	

4.2.Содержание тем дисциплины

Раздел I: ОРГАНИЗАЦИОННО-ЭКОНОМИЧЕСКИЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(РАЗВИТИЕ СИСТЕМЫ ЭКОНОМИКО-ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ НА БАЗЕ КОРПОРАТИВНЫХ МЕХАНИЗМОВ УПРАВЛЕНИЯ РИСКАМИ)

Тема 1. Введение в дисциплину и существующие подходы организационно-экономического обеспечения информационной безопасности региона

Предмет и задачи курса. Значение и место курса в подготовке магистров по информационной безопасности. Взаимосвязь курса с другими дисциплинами.

Разделы и темы, их распределение по видам аудиторных занятий. Формы проведения контрольных мероприятий. Формы проверки знаний. Состав и методика самостоятельной работы студентов по изучению дисциплины.

Знания, умения и компетенции, получаемые студентами в результате изучения курса. Рекомендованная научная и учебная литература.

Роль и место информационной безопасности в экономической сфере деятельности предприятий региона. Современное состояние проблемы по реализации управление информационными рисками для экономических объектов (международный и отечественный уровень).

Сущность и существующий уровень комплексного риск-ориентированного организационного обеспечения информационно-экономической безопасностью современных корпоративных предприятий. Цель и задачи информационно-менеджерального подхода обеспечения информационно-экономической безопасности предприятий.

Тема 2. Основные положения новых подходов организационно-экономического обеспечения информационной безопасности региона

Общая характеристика новых базовых положений по организационно-экономическому обеспечению информационной безопасности.

Концепция риска, обусловливающая принципиальные направления и аспекты применения комплексного подхода к управлению информационными рисками предприятия. Система комплексного управления рисками предприятия как ключевой корпоративный механизм

и форма обеспечения экономико-информационной безопасности на микроуровне.

Корпоративный риск-менеджмент как форма обеспечения информационно-экономической безопасности на микроуровне.

Концепция качества страхового механизма как основа решения проблемы по корпоративным информационных рискам.

Концепция контроллинга как ключевой корпоративный механизма в системе обеспечения информационно-экономической безопасностью.

Обеспечения информационно-экономической безопасности предприятий на базе интеграции корпоративных механизмов управления информационными рисками.

Математическая модель комплексной оценки экономической эффективности уровня информационной безопасности предприятий региона.

Раздел (модуль) 2. ОРГАНИЗАЦИОННО-УПРАВЛЕНЧЕСКИЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИНЯТИЯ ОРГАНИЗАЦИОННО-УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ)

Тема 3. Существующие основы обеспечения информационной безопасности принятии организационно-управленческих решений

Сущность и содержание существующих подходов по выбору модели организационного управления в условиях жесткого информационного противостояния.

Особенности функционирования социально-экономических систем с учетом механизмов информационного взаимодействия объектов финансового рынка и страховых компаний и банков. Технологии обеспечения информационной безопасности систем организационного управления экономическими объектами на основе информационных систем поддержки принятия управленческих решений.

Сущность обеспечения информационной безопасности принятии организационно-управленческих решений в современных конкурентных условиях.

Тема 4. Основные положения новых подходов по обеспечению информационной безопасности принятии региональных организационно-управленческих решений

Обзор существующей методики регулирования рисков в области

информационной безопасности поддержки принятия управленческих решений в регионе. Концептуальная методика проектирования архитектуры корпоративной системы информационной безопасности. Инсайдерские информационные риски в региональной системе обеспечения информационной безопасности. Методика организационного управления на основе информационного прогнозирования динамики изменения рисков области информационной безопасности.

Комплексный механизм принятия решений по управлению рисками основанный на: регулировании и оценке информационных потоков; формировании ситуационных центров, контроле качества активов региональных объектов.

Технологии обеспечения информационной безопасности и инструменты развития систем обмена информационными базами данных в системе принятия управленческих решений. Концептуальная схема построения интегрированной информационной системы взаимодействия региональных объектов при выработки управленческих решений в области информационной безопасности.

Принципы построения систем организационного управления рисками на основе информационной безопасности для корпоративных экономических объектов.

Требования к защите системных средств организационного управления, обеспечивающих информационную безопасность взаимодействия объектов и объективную оценку функциональной безопасности существующих средств защиты информации.

Универсальная методика обеспечения информационной безопасности, направленная на проектирование и разработку многофункциональной системы информационной поддержки принятия управленческих решений на основе формирования ситуационных центров, которая включает интегрирование в одном решении управления: информационной инфраструктуру, IT-услуги и бизнес-процессы.

Проектирование защищенной системы по преднамеренным угрозам на основе развертывания региональных ситуационных центров информационной безопасности. Схема взаимодействия компонентов системы управления информационной безопасностью на основе ситуационного центра.

5. Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине (модулю)

«Методические указания для самостоятельной работы обучающихся по освоению дисциплины» представлены в Приложении 2 к настоящей РП.

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

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине приведена в Приложении 1 к настоящей РП.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Попов Ю.И. Управление проектами: Учебное пособие / Попов Ю.И., О. В. Яковенко. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2015. - 208 с. - ISBN 978-5-16-002337-3.
URL: http://znanium.com/go.php?id=492857
2. Блау, С.Л. Инвестиционный анализ: учебник / С.Л. Блау. - М.: Дашков и Ко, 2014. - 256 с. - (Учебные издания для бакалавров). http://znanium.com/go.php?id=512662

Дополнительная литература:

3.Тихомирова О.Г. Управление проектами: практикум: учебное пособие / Тихомирова О.Г. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2016. - 273с. - ISBN 978-5-16-011601-3.
URL: http://znanium.com/go.php?id=537343

8.Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Интернет-ресурсы:

1. http://www.biblioclub.ru
2. http://znanium.com

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Методические указания для обучающихся по освоению дисциплины (модуля) приведены в Приложении 2 к настоящей рабочей программе.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- **Перечень программного обеспечения:** MSOffice, PowerPoint.

- **Информационные справочные системы:**
  1. Электронные ресурсы образовательной среды Университета..
  2. Информационно-справочные системы (Консультант+; Гарант).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Лекционные занятия:

- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций / слайдов.

Практические занятия:

- Аудитория, оснащенная мультимедийными средствами (проектор, ноутбук), демонстрационными материалами (наглядными пособиями).
- рабочее место преподавателя, оснащенное ПК с доступом в глобальную сеть Интернет ;
- рабочие места студентов, оснащенные компьютерами с доступом в глобальную сеть Интернет.

Самостоятельная работа студентов может проводится как в специально оборудованных компьютерных классах университета с выходом в Интернет, так и в домашних условиях при наличии Интернет – сети.

Приложение 1

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

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ) ЭКОНОМИКО-УПРАВЛЕНЧЕСКИЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки: 10.04.01 - Информационная безопасность

Профиль: Менеджмент информационной безопасности

Уровень высшего образования: магистратура

Форма обучения: очная

Королев
2023

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

№ п/п	Индекс компе-тенции	Содержание компетенции	Раздел дисциплины, обеспечивающий формирование компетенции	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает:		
				Трудовые действия	Необходимые умения	Необходимые знания
1.	УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.	Тема:1 - 4	К-1.3 Использует методы системного и критического анализа, анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними.	К-1.2. Определяет уязвимости и угрозы информационной безопасности, необходимые для выявления и решения проблемной ситуации, планирует мероприятия и процессы по их устранению на основе системного и междисциплинарных подходов.	УК-1.1. Ставит цель, определяет способы ее достижения, разрабатывает стратегию действия, принимает конкретные решения для ее реализации с учетом требований регуляторов в области защиты информации.
2.	ПК-2	способность к самостоятельному обучению и применению новых методов исследования в профессиональной деятельности;	Тема:1-4	ПК-2.3. Разрабатывать проекты документов по созданию защищенных технологий с оформлением технических заданий на проектирование,	ПК-2.2. Проводить предпроектное обследование с выбором перспективной технологии защиты автоматизированной ИАД с разработкой проектной	ПК-2.1. Знать нормативную базу создания и эксплуатации защищенных функциональных и обеспечивающих подсистем, методы проектирования, критерии и показатели эффективности автоматизирован

				осуществлять непосредственную разработку проектных решений по ИБ и оценку их эффективности в автоматизированной ИАС.	документации и комплексной оценкой эффективности применения автоматизированной ИАС.	ной ИАС.

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

Код компетенции	***Инструменты, оценивающие сформированность компетенции***	***Этапы и показатель оценивания компетенции***	***Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания***
УК-1 ПК-2	Доклад в форме презентации	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 4 балла;*** • ***компетенция освоена на <u>базовом</u> уровне – 3 балла;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – 2 и менее баллов***	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.
УК-1 ПК-2	***Тест***	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 90% правильных ответов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 70% правильных ответов;*** • ***компетенция освоена на <u>базовом</u> уровне – от 51% правильных ответов;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – менее 50% правильных ответов***	***Например:*** ***Проводится письменно. Время, отведенное на процедуру - 30 минут.*** ***Неявка – 0 баллов.*** ***Критерии оценки определяются процентным соотношением.*** ***Неудовлетворительно – менее 50% правильных ответов.*** ***Удовлетворительно - от 51% правильных ответов.*** ***Хорошо - от 70%.*** ***Отлично – от 90%.*** ***Максимальная оценка – 5 баллов.***
УК-1 ПК-2	Контрольная работа	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 90% правильных***	1. Проводится устно в форме защиты отчета 2.Время, отведенное на процедуру – 10 - 15 мин.

		ответов ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 70% правильных ответов;*** • ***компетенция освоена на <u>базовом</u> уровне – от 51% правильных ответов;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – менее 50% правильных ответов***	Неявка – 0. Критерии оценки: 1.Соответствие оформления требованиям (1 балл). 2. Соответствие разработанного устройства техническому заданию (1 балл) 3. Моделирование работы разработанного устройства (1 балл) 4. Качество и количество используемых источников (1 балл) 5. Правильность и полнота ответов на контрольные вопросы (1 балл) Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно после защиты – для текущего контроля. Оценка проставляется в электронный журнал.

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

Примерная тематика докладов в форме презентаций:

1. Ведущие мировые разведки и их деятельность в России.
2. Основы обеспечения безопасности информации в компьютерных системах.
3. Информационная безопасность современной России: угрозы и их отражения.
4. Информационные войны в современном мире.
2. Компьютерная преступность в экономических областях.
3. Мир XXI века: информационное противоборство.
4. Компьютерные вирусы в современных информационных системах.
5. Информационные угрозы современным экономическим объектам.
6. Информатизация России и проблема защиты информации.
7. Безопасность информации в коммерческой деятельности.
8. Разведки России – исторический аспект.
9. Мировой информационный терроризм.
10. Этика защиты информации.
11. Становление и развитие промышленного шпионажа.

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

Формой контроля знаний по дисциплине «Экономико-управленческие аспекты обеспечения информационной безопасности» являются две текущие аттестации в виде тестов и итоговая аттестация в виде экзамена.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
Согласно графика учебного процесса	тестирование	УК-1 ПК-2 ,	20 вопросов	Компьютерное тестирование ; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%***
Согласно графика учебного процесса	тестирование	УК-1 ПК-2	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%***

Согласно графика учебного процесса	Экзамен	УК-1 ПК-2	2 вопроса	Экзамен проводится в устной форме, путем ответа на вопросы. Время, отведенное на процедуру – 20 минут на каждого студента	Результаты предоставляются в день проведения экзамена	Критерии оценки: «**Отлично**»: 1. знание основных понятий предмета; 2. умение использовать и применять полученные знания на практике; 3. работа на практических занятиях; 4. знание основных научных теорий, изучаемых предметов; 5. ответ на вопросы билета. «**Хорошо**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответы на вопросы билета • неправильно решено практическое задание «У**довлетвори-тельно**»: • демонстрирует частичные знания по темам дисциплин; • незнание неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; «**Неудовлетвори-тельно**»: • демонстрирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • неумение использовать и применять

						полученные знания на практике; • не работал на практических занятиях; • не отвечает на вопросы

Итоговое начисление баллов по дисциплине осуществляется в соответствии с разработанной и внедренной балльно-рейтинговой системой контроля и оценивания уровня знаний и внеучебной созидательной активности обучающихся.

4.1. Типовые вопросы, выносимые на тестирование

Тесты используются в режиме промежуточного контроля. По форме заданий выбраны закрытые тесты (с выборочным ответом). Каждому вопросу соответствует один вариант ответа.

1. Требование безопасности повторного использования объектов противоречит:
   инкапсуляции
   наследованию
   полиморфизму

2. Предположим, что при разграничении доступа учитывается семантика программ. В таком случае на игровую программу могут быть наложены следующие ограничения:
   запрет на чтение каких-либо файлов, кроме конфигурационных
   запрет на изменение каких-либо файлов, кроме конфигурационных
   запрет на установление сетевых соединений

3. В число граней, позволяющих структурировать средства достижения информационной безопасности, входят:
   меры обеспечения целостности
   административные меры
   меры административного воздействия

4. Дублирование сообщений является угрозой:
   доступности
   конфиденциальности
   целостности

5. Самыми опасными источниками внутренних угроз являются:
   некомпетентные руководители +
   обиженные сотрудники
   любопытные администраторы

6. Для внедрения бомб чаще всего используются ошибки типа:
   отсутствие проверок кодов возврата
   переполнение буфера
   нарушение целостности транзакций

7. В число целей политики безопасности верхнего уровня входят:
   решение сформировать или пересмотреть комплексную программу безопасности
   обеспечение базы для соблюдения законов и правил
   обеспечение конфиденциальности почтовых сообщений

8. В число целей программы безопасности верхнего уровня входят:
   управление рисками
   определение ответственных за информационные сервисы
   определение мер наказания за нарушения политики безопасности

9. В рамках программы безопасности нижнего уровня осуществляются:
   стратегическое планирование
   повседневное администрирование
   отслеживание слабых мест защиты

10. Политика безопасности строится на основе:
    общих представлений об ИС организации
    изучения политик родственных организаций
    анализа рисков

11. В число целей политики безопасности верхнего уровня входят:
    формулировка административных решений по важнейшим аспектам
    реализации программы безопасности +
    выбор методов аутентификации пользователей
    обеспечение базы для соблюдения законов и правил

4.2 Типовые вопросы, выносимые на экзамен

1. Процессный подход к построению СУИБ и циклическая модель PDCA.
2. Цели и задачи, решаемые СУИБ.
3. Стандартизация в области построения СУИБ: сходства и различия стандартов.
4. Стратегии выбора области деятельности СУИБ.
5. Стратегии построения СУИБ (построение системы в целом, построение отдельных процессов управления ИБ с последующим объединением в систему).
6. Основные этапы разработки СУИБ и роль руководства организации на каждом из этапов.
7. Политика ИБ и политика СУИБ: сходства и различия.

8. Распределение ролей и ответственности в рамках СУИБ: базовая ролевая структура, дополнительные роли в рамках процессов управления ИБ.
9. Анализ рисков ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
10. Анализ рисков ИБ: основные подходы, основные этапы процесса.
11. Управление инцидентами ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
12. Расследование инцидентов ИБ: виды расследования инцидентов, критерии выбора необходимого вида расследования, основные этапы расследования (для различных видов расследования).
13. Внутренние аудиты ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
14. Анализ со стороны руководства: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
15. Обучение и обеспечение осведомленности пользователей: цели и задачи процесса, роль процесса в рамках СУИБ.
16. Внедрение процессов управления ИБ: этапы и последовательность. Ввод СУИБ в эксплуатацию: возможные проблемы и способы их решения
17. Правовые аспекты построения СУИБ организации.

Приложение 2

Методические указания для обучающихся по освоению дисциплины (модуля)

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ ЭКОНОМИКО-УПРАВЛЕНЧЕСКИЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки: 10.04.01 - Информационная безопасность

Направленность (профиль): Менеджмент информационной безопасности

Уровень высшего образования: магистратура

Форма обучения: очная

Королев
2023

1. Общие положения

Целью изучения дисциплины является формирование у обучаемых концептуальных и методологических подходов в области экономико-управленческих основ обеспечения информационной безопасности региона в процессе развития современного информационного общества.

Задачами дисциплины являются:

- раскрытие сущности, целей и содержание экономико-управленческих основ обеспечения информационной безопасности региона;
- освоение содержания базовых экономико-управленческих компонентов обеспечения информационной безопасности;
- раскрытие сущности и содержания экономико-управленческих принципов обеспечения информационной безопасности региона;
- овладение методологическими основами экономико-управленческих процессов обеспечения информационной безопасности региона;
- освоение методологии и организации процесса разработки экономико-управленческих решений в области обеспечения информационной безопасности;
- овладение методиками определения информационных рисков при реализации выработанных управленческих решений в области информационной безопасности региона;
- определение методологических подходов комплексной функциональной и экономической оценки эффективности принимаемых управленческих решений по обеспечению информационной безопасности;
- овладение методологией управления информационными рисками критериями и методами оценки эффективности проектов по обеспечению информационной безопасности;
- определение общих методологических подходов построения систем управления информационной безопасностью информационных объектов региона.

2. Указания по проведению практических занятий

Раздел 1. Концептуально-теоретические основы управления информационной безопасностью

Тема 1. Базовые основы систем и процессов управления информационной безопасностью

Практическое занятие 1.

Вид практического занятия**:** смешанная форма практического занятия.

Образовательные технологии: *групповая дискуссия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки систем и процессов управления информационной безопасностью

Учебные вопросы:

- Управление информационной безопасностью. Комплексная система управления информационной безопасностью.
- Основные определения и критерии классификации угроз. Основные угрозы доступности.
- Основные угрозы целостности.
- Основные угрозы конфиденциальности.
- Источники угроз.

Продолжительность занятия-6 часов.

Тема 2. Политика информационной безопасности отдельных структур (объектов, процессов)

Практическое занятие 2.

Вид практического занятия**:** смешанная форма практического занятия.

Образовательные технологии: *беседа.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки о политике безопасности отдельных структур

Учебные вопросы:

- Определение политики информационной безопасности
- Принципы политики безопасности
- Виды политики безопасности
- Политики безопасности для
- Уровни политики безопасности

Продолжительность занятия-6 часов.

Раздел 2. Прикладные аспекты управления информационной безопасностью

Тема 3. Организационно-кадровые и технические аспекты управления информационной безопасностью

Практическое занятие 3.

Вид практического занятия**:** смешанная форма практического занятия.

Образовательные технологии: *практическая работа в группах.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки в организационно-кадровых и технических аспектах управления информационной безопасностью

Учебные вопросы:

- Основные направления обеспечения информационной безопасности. Законодательно-правовая база обеспечения информационной безопасности на предприятии.
- Нормативные акты предприятия по информационной безопасности.
- Формы правовой защиты информации на предприятии.

Продолжительность занятия-6 часов.

Тема 4. Основы оценки эффективности управления информационной безопасностью

Практическое занятие 4.

Вид практического занятия**:** смешанная форма практического занятия.

Образовательные технологии: *групповая дискуссия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки оценки эффективности управления ИБ

Учебные вопросы:

- Метод оценки рисков на основе модели информационных потоков.
- Расчет рисков по угрозе конфиденциальность.
- Расчет рисков по угрозе целостность.
- Методы оценивания информационных рисков.
- Табличные методы оценки рисков.
- Разделение рисков на приемлемые и неприемлемые.

Продолжительность занятия-6 часов.

3. Указания по проведению лабораторного практикума

Не предусмотрено учебным планом

4. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	Базовые основы систем и процессов управления информационной безопасностью	***Подготовка докладов и презентаций по темам:*** Место информационной безопасности в системе национальной безопасности. Современная концепция информационной безопасности. Цели и концептуальные основы защиты информации.
2.	Политика информационной безопасности отдельных структур (объектов, процессов)	***Подготовка докладов и презентаций по темам:*** Критерии, условия и принципы отнесения информации к защищаемой. Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности. Модель угроз.
3	Организационно-кадровые и технические аспекты управления информационной безопасностью	***Подготовка докладов и презентаций по темам:*** Понятие и структура угроз защищаемой информации. Источники, виды и методы дестабилизирующего воздействия на защищаемую информацию. Каналы и методы несанкционированного доступа к конфиденциальной информации.
4	Основы оценки эффективности управления информационной безопасностью	***Подготовка докладов*** *и презентаций* ***по темам:*** Критерии оценки безопасности информационных технологий. Методы защиты информации от несанкционированного доступа. Риски информационной безопасности.

5. Указания по проведению контрольных работ для обучающихся очной формы обучения

5.1. Требования к структуре.

Структура контрольной работы должна способствовать раскрытию темы: иметь титульный лист, содержание, введение, основную часть, заключение, список литературы.

5.2. Требования к содержанию (основной части).

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.
2. При определении целей и задач исследования необходимо правильно их формулировать. Так, в качестве цели не следует употреблять глагол «сделать». Правильно будет использовать глаголы: «раскрыть», «определить», «установить», «показать», «выявить» и т.д.
3. Основная часть работы включает 2 - 4 вопроса, каждый из которых посвящается решению задач, сформулированных во введении, и заканчивается констатацией итогов.
4. Приветствуется иллюстрация содержания работы таблицами, графическим материалом (рисунками, схемами и т.п.).
5. Необходимо давать ссылки на используемую литературу.
6. Заключение должно содержать сделанные автором работы выводы, итоги исследования.
7. Вслед за заключением идет список литературы, который должен быть составлен в соответствии с установленными требованиями. Если в работе имеются приложения, они оформляются на отдельных листах, и должны быть соответственно пронумерованы.

5.3. Требования к оформлению.

Объём контрольной работы – … страниц формата А4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

6. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Попов Ю.И. Управление проектами: Учебное пособие / Попов Ю.И., О. В. Яковенко. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2015. - 208 с. - ISBN 978-5-16-002337-3.
URL: http://znanium.com/go.php?id=492857
2. Блау, С.Л. Инвестиционный анализ: учебник / С.Л. Блау. - М.: Дашков и Ко, 2014. - 256 с. - (Учебные издания для бакалавров). http://znanium.com/go.php?id=512662

Дополнительная литература:

3.Тихомирова О.Г. Управление проектами: практикум: учебное пособие / Тихомирова О.Г. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2016. - 273с. - ISBN 978-5-16-011601-3.
URL: http://znanium.com/go.php?id=537343

7.Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Интернет-ресурсы:

3. http://www.biblioclub.ru
4. http://znanium.com

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- **Перечень программного обеспечения:** MSOffice, PowerPoint.

- **Информационные справочные системы:**

1. Электронные ресурсы образовательной среды Университета..
2. Информационно-справочные системы (Консультант+; Гарант).