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 ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И УПРАВЛЯЮЩИХ СИСТЕМ

РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.09 «ТЕОРИЯ СИСТЕМ И СИСТЕМНЫЙ АНАЛИЗ»

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: Логачева Н.В. Рабочая программа дисциплины (модуля): Теория систем и системный анализ. Королев МО: «Технологический Университет», 2023

Рецензент: Артюшенко В.М.

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки магистров 10.04.01 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)	Артюшенко В.М. д.т.н., проф.			
Год утверждения (переутверждения)	2023	2024		
Номер и дата протокола заседания кафедры	№12 от 05.04.2023г.			

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 (модулю), соотнесенных с планируемыми результатами освоения ОПОП

Целью изучения дисциплины «Теория систем и системный анализ» является совершенствование подготовки и повышение квалификации кадров в сфере информационно-технологических дисциплин для преподавательской деятельности и применения современных образовательных технологий; обучение методам *познания, анализа, структурирования моделей процессов и объектов, а также методологии формализации задачи принятия решений* для **достижения** определенной **цели**, для которой создается (выделяется) некоторая *искусственная система*; а также умение применять эти знания при решении конкретных задач.

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

Универсальные компетенции:

- УК-2: Способен управлять проектом на всех этапах его жизненного цикла.

Профессиональные компетенции:

- ПК-1: Способен организовывать выполнение работ, управлять коллективом автоматизированных ИАС в защищенном исполнении.

Показатель освоения компетенции отражают следующие индикаторы:

Трудовые действия:

- УК-2.3 Формулирует, на основе поставленной проблемы проектную задачу и способы ее решения через реализацию проектного управления, разрабатывает и реализует проекты.

- ПК-1.3. Управлять работой коллектива профессионалов ИБ, разрабатывать нормативно-методические документы по функционированию автоматизированной ИАС, формировать комплекс мер по информационной защите автоматизированной ИАС с разработкой частных политик безопасности компьютерных систем.

Необходимые умения:

- УК-2.2. Разрабатывает тактико-технические требования, техническое задание по реализации проекта в рамках обозначенной проблемы, определяет целевые этапы, основные направления работ, объясняет цели и формулирует задачи, связанные с подготовкой и реализацией проекта.

- ПК-1.2. Работать в коллективе, разрабатывать организационно-управленческие документы, принимать управленческие решения, реализовывать целесообразные меры противодействия информационным угрозам с применением национальных и международных стандартов в области ЗИ, оценивать их эффективность.

Необходимые знания:

- УК-2.1. Разрабатывает план реализации проекта с использованием инструментов планирования и управляет проектом, оценивает потребности в

ресурсах, осуществляет мониторинг хода реализации проекта, корректирует отклонения, вносит дополнительные изменения в план реализации проекта и оценивает эффективность проекта.

- ПК-1.1. Знать научные основы, методы и технологии управленческой деятельности, нормативную базу по созданию и эксплуатацию защищенных автоматизированных ИАС, принципы и методы организации работ по ЗИ в ИАС, основные средства и способы организационного обеспечения ИБ, источники и классификацию угроз ИБ.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП ВО

Дисциплина «Теория систем и системный анализ» относится к обязательной части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки магистров по направлению подготовки «Информационная безопасность».

Дисциплина базируется на ранее изученных дисциплинах: «Теоретические основы управления», «Современная философия и методология науки» и компетенциях: ПК-1, 2; УК-2;

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для написания магистерской диссертации.

3.Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 часа

Таблица 1

Виды занятий и контроля	Всего часов	Семестр 3
Общая трудоемкость, час.	**72**	**72**
ОЧНАЯ ФОРМА ОБУЧЕНИЯ		
Аудиторные занятия	**38**	**38**
Лекции (Л)	16	16
Практические занятия (ПЗ)	16	16
Другие виды контактной работы*	**6**	**6**
Самостоятельная работа.	**34**	**34**
Вид итогового контроля	**Зачет**	**Зачет**

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

4. Содержание дисциплины

4.1. Темы дисциплины и виды занятий

Таблица 2

№ п/п	Наименование тем дисциплины	Лекции, час	Практич. занятия. час.	Занятия в интерактивной форме, час	Код компетенций
1	Тема 1 Понятия о системном подходе, системном анализе.	2	2	2	УК-2
2	Тема 2. Системы и закономерности их функционирования и развития.	2	2	1	УК-2 ПК-1
3	Тема 3. Классификация систем.	2	2	1	ПК-1
4	Тема 4. Поведение, деятельность и организация систем.	2	2	1	УК-2 ПК-1
5	Тема 5. Свойства системы.	2	2	1	ПК-1
6	Тема 6.Системное моделироване.	2	2	1	УК-2 ПК-1
7	Тема 7.Модели систем.	4	4	1	УК-2 ПК-1
	Итого:	**16**	**16**	**8**	

4.2. Содержание тем дисциплины

Тема 1. Понятия о системном подходе, системном анализе.
Выделение системы из среды, определение системы. Оптимизация систем и системное проектирование.
Тема 2. Системы и закономерности их функционирования и развития. Системный подход как методология управления сложными системами. Управляемость, достижимость, устойчивость.
Тема 3. Классификация систем.
Естественные, концептуальные и искусственные, простые и сложные, целенаправленные, целеполагающие, активные и пассивные, стабильные и развивающиеся системы.
Тема 4. Поведение, деятельность и организация систем.
Особенности применения обобщенного алгоритма . Формирование и анализ моделей. Выявление топологии системы.
Тема 5. Свойства системы.
Целостность и структуризация, связность, структура, организация, интегрированные качества.
Тема 6. Системное моделирование.

Основные проблемы теории систем. Модели и моделирование. Управление системой.

Тема 7. Модели систем.

Обоснование класса допустимых систем. Статические, динамические, концептуальные, формализованные (процедуры формализации моделей систем), информационные, логико-лингвистические, семантические и др.

Роль человека в решении задач системного анализа.

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

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

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.

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

Основная литература:

1.Теория систем и системный анализ : учебник / С.И. Маторин, А.Г. Жихарев, О.А. Зимовец, М.Ф. Тубольцев, А.А. Кондратенко; под ред. С. И. Маторин. - Москва|Берлин : Директмедиа Паблишинг, 2020. - 509 с. : 509. - ISBN 978-5-4499-0675-5.
URL: http://biblioclub.ru/index.php?page=book&id=574641

2.Самойленко, А. П. Информационные технологии статистической обработки данных : учебное пособие / А.П. Самойленко, О.А. Усенко; Министерство образования и науки Российской Федерации; Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет»; Инженерно-технологическая академия. - Ростов-на-Дону|Таганрог : Издательство Южного федерального университета, 2017. - 127 с. : ил. - ISBN 978-5-9275-2521-8. - Электронная программа (визуальная). Электронные данные : электронные.
URL: http://biblioclub.ru/index.php?page=book&id=500042

Дополнительная литература:

3.Бродовская, Е. В.Большие данные в исследовании политических процессов : учебное пособие / Е.В. Бродовская, А.Ю. Домбровская; Министерство науки и высшего образования Российской Федерации; Московский педагогический государственный университет. - Москва : МПГУ, 2018. - 88 с. : схем., табл., ил. - ISBN 978-5-4263-0712-4. - Текст (визуальный) : непосредственный.
URL: http://biblioclub.ru/index.php?page=book&id=563578

4.Аврунев, О. Е.Модели баз данных : учебное пособие / О.Е. Аврунев, В.М. Стасышин; Новосибирский государственный технический университет. - Новосибирск : Новосибирский государственный технический университет, 2018. - 124 с. : ил., табл. - ISBN 978-5-7782-3749-0.
URL: http://biblioclub.ru/index.php?page=book&id=575324
5.Голиков А. М. Тестирование и диагностика в инфокоммуникационных системах и сетях: курс лекций, компьютерные лабораторные работы и практикум, задание на самостоятельную работу; учебное пособие / А.М. Голиков. - Томск: ТУСУР, 2016. -436 с. - (Учебная литература для вузов).
URL: http://biblioclub.ru/index.php?page=book&id=480803

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-справочная система (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:

- компьютерный класс с проектором для интерактивного обучения и проведения лекций в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная

система не ниже WindowsXP; офисные программы MSOffice 7; программы эмуляции виртуальных машин (VM-vare, VM-box или др.); операционная система MS Windows Server 2003 или др. сетевая ОС.

- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в 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 ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И УПРАВЛЯЮЩИХ СИСТЕМ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ
ТЕОРИЯ СИСТЕМ И СИСТЕМНЫЙ АНАЛИЗ

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 компетенции	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-2	Способен управлять проектом на всех этапах его жизненного цикла.	Тема:1,2,3,4,5,6,7	УК-2.3 Формулирует, на основе поставленной проблемы проектную задачу и способы ее решения через реализацию проектного управления, разрабатывает и реализует проекты.	УК-2.2. Разрабатывает тактико-технические требования, техническое задание по реализации проекта в рамках обозначенной проблемы, определяет целевые этапы, основные направления работ, объясняет цели и формулирует задачи, связанные с подготовкой и реализацией проекта.	УК-2.1. Разрабатывает план реализации проекта с использованием инструментов планирования и управляет проектом, оценивает потребности в ресурсах, осуществляет мониторинг хода реализации проекта, корректирует отклонения, вносит дополнительные изменения в план реализации проекта и оценивает эффективность проекта.
2.	ПК-1	Способен организовывать выполнение работ, управлять коллективом автоматизированных ИАС в защищенном исполнении	Тема:1,2,3,4,5,6,7	ПК-1.3. Управлять работой коллектива профессионалов ИБ, разрабатывать нормативно-методические документы по функционированию автоматизированной ИАС, формировать комплекс мер по информационной защите автоматизированной ИАС с разработкой частных политик безопасно-	ПК-1.2. Работать в коллективе, разрабатывать организационно-управленческие документы, принимать управленческие решения, реализовывать целесообразные меры противодействия информационным угрозам с применением национальных и международных стандартов в области ЗИ, оценивать их	ПК-1.1. Знать научные основы, методы и технологии управленческой деятельности, нормативную базу по созданию и эксплуатацию защищенных автоматизированных ИАС, принципы и методы организации работ по ЗИ в ИАС, основные средства и способы организационного обеспечения ИБ, источ-

				сти компьютерных систем.	эффективность.	ники и классификацию угроз ИБ.

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-2 ПК-1	***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-2 ПК-1	Доклад в форме презентации	***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***	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-2 ПК-1	Контрольная работа	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 90% правильных ответов*** ***Б) частично сформирована:*** • ***компетенция***	1. Проводится устно в форме защиты отчета 2.Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие оформления требованиям

		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***	(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

3.1 Примерная тематика докладов в форме презентаций:

1. Общая характеристика принципов, методов и механизмов обеспечения компьютерной безопасности. Основы обеспечения безопасности информации в компьютерных системах.

2. Исследование объекта защиты информации и анализ его защищённости по видам угроз, классам каналов несанкционированного получения информации, причинам нарушения целостности информации и потенциально возможным злоумышленным действиям.

3. Проектирование архитектуры системы защиты информации выбранного объекта и оценка его уровня защищённости.

4. Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников.

5. Совершенствование системы защиты информации предприятия (фирмы) на основе комплексного применения современных средств защиты информации.

6. Разработка и обоснование требований к системе защиты информации предприятия (фирмы) и рекомендаций по её эффективному наращиванию.

7. Направления повышения эффективности существующей системы защиты и методика применения средств защиты информации на выбранных объектах исследования.

8. Разработка проекта создания системы защиты информации на выбранных типовых офисных объектах.

9. Основные виды атак на компьютерные системы (КС), их классификация, проблемы обеспечения информационной безопасности в проводных КС.

10. Беспроводной доступ к локальным сетям. Угрозы и уязвимости в беспроводных компьютерных системах.

11. Компьютерная преступность в экономических областях.

12. Компьютерные вирусы в современных информационных системах.

13. Информационные угрозы современным экономическим объектам.

14. Безопасность информации в коммерческой деятельности.

15. Становление и развитие промышленного шпионажа.

16. Модель распространения прав доступа Take-Grant. Цель использования модели Take-Grant. Основные элементы модели Take-Grant. Формальное описание модели Take-Grant.

17. Описание систем защиты с помощью матрицы доступа. Таблицы, описывающие права доступа субъектов к объектам. Описание модели Харрисона-Руззо-Ульмана (HRU).

18. Направления повышения эффективности существующей системы защиты и методика применения средств защиты информации на выбранных объектах исследования.

19. Общий подход к построению систем, реализующих мандатную (полномочную) политику безопасности в модели BL (Белла-Лападулы).

20. Назначение модели Белла-Лападулы. Описание модели Белла-Лападулы (BL). Основная теорема безопасности модели Белла-Лападулы.

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

Формой контроля знаний по дисциплине «Теория систем и системный анализ» являются две текущие аттестации в виде тестов и итоговая аттестация в виде зачета.

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
Проводится в сроки, установленные графиком образовательного процесса	тестирование	УК-2 ПК-1	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%***
Проводится в сроки, установленные графиком образовательного процесса	тестирование	УК-2 ПК-1	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%***
Проводится в сроки, установленные графиком образовательного процесса	Зачет	УК-2 ПК-1	3 вопроса	Зачет проводится в письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	Результаты предоставляются в день проведения зачета	Критерии оценки: **«Зачтено»:** • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на семинарских занятиях; • знание основных научных теорий, изуча-

						емых предметов; • ответ на вопросы билета. **«Не зачтено»**: демонстрирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • неумение использовать и применять полученные знания на практике; • не работал на семинарских 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.

Вопросы, выносимые на зачет

1. Выстройте по критерию строгости следующие понятия: инструкция, методика, алгоритм.
2. Приведите примеры алгоритмизации творческой деятельности человека.
3. Дайте определение механизма.
4. Дайте определение автомата.
5. В чем состоит базовый принцип кибернетики?
6. Перечислите классические типы обратных связей в системах и дайте им определения.
7. Приведите примеры различных типов обратных связей в экономических системах.
8. Что такое управление?
9. В чем заключается сложность управления системой?
10. В чем причины возникновения синтетического и аналитического образа человеческого мышления?
11. Раскройте сущность аналитического подхода к исследованию системы и приведите примеры.
12. Перечислите основные функции финансовой системы предприятия.

13. В чем заключается методологическая основа системного анализа зарождения системы?
14. Назовите характерные особенности неорганизованной среды.
15. Каким числом степеней свободы характеризуется хаос?
16. Как осуществляется специализация элементов формирующейся системы?
17. Дайте определение бифуркации.
18. Что изучает теория катастроф?
19. В чем заключается развитие системы?
20. В чем заключается самоорганизация системы?
21. Назовите основные причины гибели системы.
22. Приведите наиболее вероятные варианты деформации каналов связи между элементами системы.
23. В чем состоит источник развития системы?
24. Приведите наиболее действенные способы разрушения системы.
25. Перечислите и интерпретируйте основные свойства системы.
26. Что такое эмерджентность системы?
27. В чем заключается сущность редукционизма и чем он отличается от системного подхода?
28. Как взаимосвязаны понятия «страта» и «иерархия»?
29. В чем заключается разница между внешними и внутренними связями системы?
30. Какое свойство лежит в основе деления систем на открытые и закрытые?
31. С помощью чего обеспечивается устойчивость системы?
32. В чем заключаются внутренняя и внешняя цели системы?
33. Приведите примеры эквифинальности естественных, искусственных и смешанных систем.
34. Назовите ключевой признак в классификации систем.
35. В чем заключается целевой характер классификации систем?
36. Перечислите классы систем по описанию входных и выходных потоков.
37. Перечислите классы систем по типу внутреннего операторы (преобразователя) системы.
38. Перечислите классы систем по способу управления ими.
39. Перечислите классы систем по степени ресурсной обеспеченности внутреннего оператора.
40. Что лежит в основе деления системы на большие и малые, сложные и простые?
41. Что является главной задачей в деятельности системного аналитика?
42. Перечислите основные стадии построения модели проблемной ситуации.
43. Приведите состав и содержание работ системного аналитика на стадии анализа проблемы.

44. Приведите состав и содержание работ системного аналитика на стадии синтеза модели проблемы.
45. Перечислите методы проверки адекватности модели исследуемой области.
46. Что представляет собой критериальная функция?
47. Как увязываются между собой метод поиска критериальной функции и тип модели проблемной ситуации?
48. Как классифицируются методы, используемые для описания проблемных ситуаций?
49. Существует ли строгое разделение между классами методов, используемых для описания проблемных ситуаций?
50. В чем заключается ключевая проблема моделирования экономических систем?
51. Как классифицируются модели систем относительно времени?
52. Дайте определение модели «черного ящика».
53. Постройте модель «черного ящика» с целью определения состава информационной базы чужого ПК.
54. Дайте определение состава модели.
55. Какой набор структурных компонент применяется для построения модели состава?
56. Что такое уровень элементарности в системном анализе?
57. Какими рамками ограничена модель состава системы?
58. Какими причинами обусловлена множественность вариантов модели состава системы?
59. Сформулируйте определение структуры системы.
60. Какая роль отведена структуре системы на ее жизненном пути?
61. Сформулируйте определение для структурной модели системы.
62. Как изменяется число связей в системе с увеличением числа ее элементов?
63. Что такое формальная модель системы и как она используется при построении моделей реальных систем?
64. Приведите математическую запись процессов динамической модели «черного ящика».
65. Дайте определение безинерционной системы.
66. Дайте определение памяти системы.
67. Приведите примеры систем, процессов или явлений, в которых невозможно исправить пагубное развитие ситуации.
68. В чем заключается сложность моделирования системы с запаздыванием?
69. Какие виды динамики изучает теория систем?
70. В чем заключается функционирование системы?
71. Что изучает экономический анализ?
72. Что является методологической основой экономического анализа?
73. Как фиксируется состояние динамической системы?
74. Что такое «траектория системы» и как она задается?

75.Как задаются граничные состояния системы?

4.1 Перечень тем для опроса

1.Основные понятия и определения системы, среды, цели, проблемы, функций, структур, ресурсов.

2.Модели описания сложных систем.

3.Основные этапы системной деятельности, алгоритмы анализа и синтеза систем, метод «дерева целей».

4.Функциональные характеристики сложных систем: эффективность, надежность, качество управления, сложность.

5.Модели управления, классификация.

6.Проблемы разработки и применения методов системного анализа сложных прикладных объектов исследования.

7.Основы методологии системного подхода к изучению сложных объектов, методы синтеза сложных технических систем.

8.Понятие и определение цели системы, виды и формы представления структур целей, методики определения целей и функций систем управления.

9.Иерархические принципы построения систем.

10. Методы системного моделирования, принятия решений в сложных системах, использование математических методов в теории систем.

11. Информационный подход к анализу систем.

12. Методы организации сложных экспертиз.

13. Анализ информационных ресурсов.

14. Развитие систем организационного управления.

15. Основные характеристики моделей данных.

16. Основные характеристики моделей данных.

17. Информационно-логические модели данных.

18. Методы обработки экспериментальных данных.

19. Методы передачи и хранения информации.

20. Методы сжатия изображений, цифровая обработка данных.

21. Методы защиты информации в сетях передачи данных.

22. Понятие состояния.

23. Марковские модели процессов.

24. Деревья состояний.

25. Уравнения состояний линейных моделей динамических систем.

26. Понятие управляемости и наблюдаемости динамических систем.

27. Функционирование систем в условиях неопределенности, управление в условиях риска.

28. Микропроцессоры в технических системах.

29. Оптимизация управления и принятия решений с целью повышения эффективности функционирования объектов исследования.

30. Целенаправленные воздействия человека на объекты исследования.

31. Проблемы адаптивного синтеза информационно-вычислительных конфигураций.

32. Комплексные методы повышения эффективности, надежности и ка-

чества функционирования технических систем.

33. Прикладные исследования системных связей и закономерностей функционирования, ориентированные на повышение эффективности управления с использованием современных методов обработки информации.

34. Разработка программно-аппаратных комплексов управления.

4.2 Перечень тем для самостоятельной работы

1 Анализ жизненного цикла сложных технических систем, принятие решений о модернизации.

2 Классификация моделей технических объектов.

3 Основные этапы построения математических моделей аналитическим способом.

4 Структурных подход к построению моделей технических систем.

5 Анализ качества модели, выбор наилучшей структуры модели из заданной совокупности структур.

6 Этапы предэкспериментальной подготовки: изучение объекта, постановка задачи исследования.

7 Сущность процесса имитационного моделирования, среда моделирования, разработка прикладных приложений.

8 Расчет надежности, диагностика и прогнозирование состояний.

9 Системный анализ и иерархия целей инженерно-технических задач.

10 Прикладные задачи принятие решений в условиях риска и неопределенности.

11 Основные этапы анализа данных в задаче математического моделирования.

12 Алгоритмы качественного и количественного анализа данных, формирование массива информативных признаков объекта исследования.

13 Обработка и передача данных в компьютерных системах.

14 Угрозы и факторы, влияющие на безопасность информации в сетях передачи данных.

15 Связь управления с обучаемостью системы.

16 Роль обратной связи в управлении.

17 Роль информации при принятии решений.

18 Принятие решений в условиях определенности и дефицита информации.

19 Методы компенсации дефицита информации.

20 Байесовский подход к принятию решений.

21 Использование игровых методов принятия решений.

22 Принцип Лапласа, применение максиминных, минимаксных и промежуточных решений.

23 Инновационный подход при управлении и совершенствовании больших систем и бизнес-плане как инструменте планирования нововведений.

24 Построение и анализ деревьев цели и систем и их взаимодействие.

4.3. Перечень тем практических работ

1. Решение задач на векторную оптимизацию.
2. Решение задач по теории планирования эксперимента.
3. Решение задач на приложения нечеткой логики.
4. Построение моделей, заданных линейных и нелинейных систем.
5. Анализ наблюдаемости и управляемости заданных систем.
6. Анализ устойчивости заданных дискретных и непрерывных линейных систем.
7. Построение робастных наблюдателей состояний

На выполнение одной работы отводится не менее одного часа. После выполнения каждой лабораторной работы обучаемый должен представить отчет о ее выполнении, а также, по указаниям преподавателя, выполнить дополнительные практические задания по теме лабораторной работы.

4.4. Контрольные вопросы и задания

Задание 1. В схеме, представленной на рисунке 1, заполните недостающие блоки

Рисунок 1 - Взаимосвязь теории и объекта системного анализа

Задание 2. Найдите соответствие

Семиотический подход	методы поиска оптимальных решений, основу которых составляют формализованные (т.е. представленные в виде конечного алгоритма) эвристики
Эвристическое программирование	разрабатывается симулятор исследуемой предметной области для проведения различных экспериментов
Метод аналогий	на практике аналитических представлений для отображения сложных систем следует иметь в виду, что они требуют установления всех детерминированных взаимосвязей между учитываемыми компонентами и целями системы в виде аналитических зависимостей.
Аналитические методы	сущность метода состоит в разработке типовых решений (например, типовой организационной структуры управления персоналом) и определении границ и условий их применения
Имитационное моделирование	информационные системы связаны с процессами обработки информации и информационного обмена

Задание 3. На рисунке 2 представлена модель. Определите, ее название: структурная модель системы, модель управления персоналом, модель взаимодействия систем, модель распределенной системы

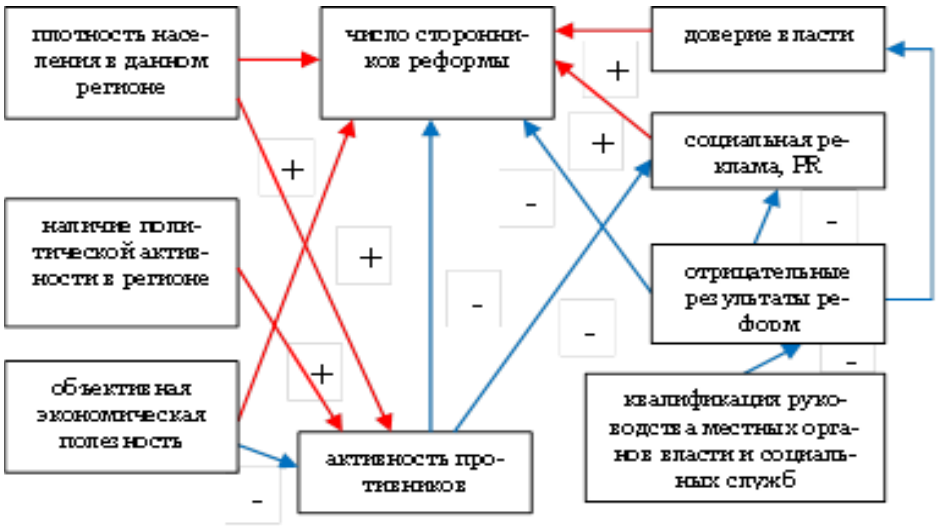


Рисунок 2 – Пример базовой модели систем _____

Типовые вопросы, выносимые на тестирование

6 семестр:

Вариант 1 (Т-1)

1. Чем различаются объект и субъект?

(?) Субъект – пассивный участник направленной деятельности, объект – активный участник направленной деятельности.

(?! Объект – пассивный участник направленной деятельности, субъект – активный участник направленной деятельности.

(?) Объект может влиять на субъект, но не наоборот.

(?) Субъект никак не отличается от объекта.

2. Что такое осознанная потребность, соотнесенная с конкретным результатом её удовлетворения.

(?) Цель

(?) Задача

(?) Желание

(?) Необходимость

3. Разность между желаемым и существующим, ликвидация которой не является очевидной это?

(?) Объективная проблема

(?) Субъективная проблема

(?) Цель

(?) Желание

4. Можно ли прировнять определения желания и цели?

(?) Да

(?) Нет

(?) Цель может стать желанием.

(?) Желание носит целевой характер, но это цель без критического осмысления её достижения.

5. Известно, что выбор цели сугубо субъективен. Что тогда является субъектом целеполагания?

(?) Точка зрения

(?) Цель

(?) Проблема

(?) Потребность

6. Что из указанного является целью-направлением?

(?) Увеличение выпуска продукции в два раза

(?) Повышение образовательного уровня работников

(?) Устранение выявленных угроз безопасности за пять недель.

(?) Строительство тридцати киосков с мороженым в тридцати конкретных городах.

7. Для чего используют критерии?

(?) Для качественной оценки степени достижения цели.

(?) Для количественной оценки степени достижения цели.

(?) Для оценки разницы между целью и достигнутым результатом

(?) Для оценки затрат на достижение цели.

8. Достаточно ли одного критерия для адекватной оценки цели?

(?) Да

(?) Нет

(?) Зависит от критерия

(?) Только для первичной оценки

9. С позиции кого/чего цель определяется как наблюдение за объектом, его исследование, анализ и описание.

(?) Цель с позиции субъекта

(?) Цель с позиции объекта

(?) Общая цель субъекта и объекта

(?) Верного ответа нет

10. С позиции кого/чего цель определяется как полноценное функционирование, способное противостоять внешним угрозам.

(?) Цель с позиции объекта

(?) Цель с позиции субъекта

(?) Цель с позиции злоумышленника

(?) Цель с позиции незаинтересованных лиц

11. Решение исходной проблемы чаще всего приводит к образованию совокупности проблем в окружающих систему объектах. Какой термин применяется для обозначения данной совокупности?

(?) Ошибка целеполагания

(?) Неправильная методика

(?) Проблематика

(?) Ложный путь решения проблемы

12. При решении любой проблемы всегда есть определенный круг «заинтересованных лиц», кто заинтересован в решении проблемы или не заинтересован. Каждая из сторон имеет свое видение проблемы и отношение к ней. Кто из перечисленных НЕ входит в круг «заинтересованных лиц».

(?) Все указанные являются заинтересованными

(?) Заказчик

(?) Налоговая инспекция

(?) Жители города

13. Как графически можно отобразить влияние решения проблем на другие объекты/субъекты?

(?) Нарисовать круг заинтересованных лиц

(?) Построить пирамиду важности влияния

(?) Построить матрицу проблематики

(?) Построить диаграмму влияний

14. Особенность цели, заключающаяся в том, что полученные результаты будут отличаться от запланированных целей, это…?

(?) Появление новой цели при её достижении

(?) Цель всегда чётко определена

(?) Цель всегда несет в себе элементы неопределенности

(?) Особенности целей зависят от конкретных задач

15. Что называется несоответствием желаемого и действительного?

(?) Проблема

(?) Обратная связь

(?) Анализ

(?) Ограничение

16. Что из перечисленного является субъектом информационной безопасности банка?

(?) Человек

(?) Компьютер

(?) Банк

(?) Программа обработки данных в ЦОД

Практическое задание (вариант)

«Решение ситуационных задач по теме: «Информационные преступления в сфере компьютерной информации и меры защиты от них»

Теоретическая часть:

Алгоритм решения задачи включает в себя следующую последовательность действий:

1. Ответ на поставленный вопрос;

2. Законодательная (нормативная) база;

3. Обоснование решения со ссылкой на соответствующие законодательные предписания и фактические обстоятельства дела (фабулу).

В качестве образца предлагается решение задачи:

В деянии Шатурина можно усмотреть признаки состава преступления, предусмотренные ст. 274 УК РФ «нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей ». законодательная база для решения задачи – ст. 274 УК РФ, примечания к ст. 272 УК РФ.

Родовым объектом данного преступления являются общественная безопасность и общественный порядок; видовым – отношения в сфере компьютерной безопасности. Непосредственный объект – это отношения, обеспечивающие правила эксплуатации хранения, обработки, передачи компьютерной информации и информационно-телекоммуникационных сетей.

Объективная сторона преступления сконструирована в качестве материального состава. Обязательные условия наступления уголовной ответственности – причинение крупного ущерба. В деянии Шатурина усматриваются отдельные признаки объективной стороны деяния, в частности, нарушения правил эксплуатации информационно-телекоммуникационных сетей. Он также обладает признаками субъекта данного преступления – вменяем и достиг 16 лет. Субъективная сторона преступления характеризуется виной как в форме умысла, так и неосторожности.

Однако, вопрос об уголовной ответственности Шатурина зависит от того, в каком размере был причинен ущерб его деянием, так как состав преступления является материальным. Согласно примечанию к ст. 22 УК РФ крупным ущербом в статьях данной главы признается ущерб сумма которого превышает один миллион рублей. Таким образом, Шатурин будет подлежать уголовной ответственности по ч. 1 ст. 274 УК РФ, если его деянием причинен ущерб на сумму свыше одного миллиона рублей.

Задачи:

1. Студент заочного отделения Шатурин решил использовать компьютер из компьютерного класса университета для оформления контрольных и курсовых работ. Без разрешения деканата факультета он проник в класс и стал работать на компьютере. Из-за крайне поверхностных знаний и навыков работы на компьютере произошли сбои в работе машины, что привело в дальнейшем к отключению модема - одного из элементов компьютерной системы.

Подлежит ли уголовной ответственности Шатурин? Дайте анализ состава преступления, предусмотренного ст.274 УК РФ. Что понимается под информационно-телекоммуникационными сетями и оконечным оборудованием в смысле ст. 274 УК РФ? Какие виды оконечного оборудования возможны? Относится ли к оконечному оборудованию телефонный модем?

1. Аспирант университета Хохлов, 23-ти лет, занимался исследовательской работой по компьютерной "вирусологии". Целью работы было выяснение масштаба глобальной сетевой инфраструктуры. В результате ошибки в механизме размножения вирусы, так называемые "сетевые черви", проникли в университетскую компьютерную сеть и уничтожили информацию, содержащуюся в компьютерах факультетов и подразделений. В результате этого были полностью уничтожены списки сотрудников университета, расчеты бухгалтерии по зарплате, повреждены материалы научно-исследовательской работы, в том числе "пропали" две кандидатские и одна докторская диссертации.

Решите вопрос о правомерности действий Хохлова. В чем заключается субъективная сторона преступлений в сфере компьютерной информации?

1. Левченко и другие граждане Российской Федерации вступили в сговор на похищение денежных средств в крупных размерах, принадлежащих "City Bank of America", расположенного в г. Нью-Йорке. Образовав устойчивую преступную группу, они в период с конца июня по сентябрь 2012 г., используя электронную компьютерную систему телекоммуникационной связи "Интернет" и преодолев при этом несколько рубежей многоконтурной защиты от несанкционированного доступа с помощью персонального компьютера стандартной конфигурации из офиса предприятия, находящегося в г. Санкт-Петербурге, вводили в систему управления наличными фондами указанного банка ложные сведения. В результате этих операций было осуществлено не менее 40 переводов денежных средств на общую сумму 10 млн 700 тыс. 952 доллара США со счетов клиентов названного банка на счета лиц, входящих в состав преступной группы, проживающих в шести странах: США, Великобритании, Израиле, Швейцарии, ФРГ, России.

Дайте уголовно-правовую оценку действиям Левченко и других членов организованной группы.

1. Студент технического вуза Иванченко во время занятий по информатике подключился к сети "Интернет" и регулярно получал в течение семестра материалы разного содержания, в том числе и сексуального характера. В конце семестра в институт поступил запрос о работе в "Интернет" и пришел чек на оплату 105 часов пребывания в сети "Интернет".

Руководство института поставило вопрос о привлечении Иванченко к уголовной и гражданской ответственности.

Дайте правовую оценку действиям студента Иванченко.

1. Оператор ЭВМ одного из государственных учреждений Утевский, используя многочисленные дискеты с информацией, получаемые от сотрудников других организаций, не всегда проверял их на наличие "вирусов", доверяясь заверениям поставщиков о том, что "вирусов" нет. В результате этого в компьютер Утевского, а затем и в компьютерную сеть учреждения попал комбинированный вирус, что привело к утрате информации, содержащей государственную тайну, и поставило под угрозу срыва запуск одного из космических объектов.

Дайте юридический анализ действий Утевского. Что следует понимать под тяжкими последствиями нарушении правил эксплуатации информационно-телекоммуникационных сетей?

1. Савченко осуществлял рассылку подложных электронных писем с целью завладения персональной информацией клиентов «Ситибанка». Рассылка представляла собой электронное письмо с сообщением о переводе 100 долларов США на личный счет клиента и содержала просьбу зайти в систему Интернет-бакинта «CitibankOnline» для подтверждения перевода. В случае следования по указанной ссылке происходило попадание на сайт, созданный Савченко, и очень похожий на стартовый экран «CitibankOnline». Десять человек ввели номер кредитной карты и пин-код для того, чтобы войти в систему. Воспользовавшись полученной таким образом информацией, Савченко совершил завладение денежными средствами Павлова и Костенко, находящимися в Ситибанке, в сумме 15 и 20 тысяч долларов соответственно.

Квалифицируйте содеянное Савченко.

1. Гуляшов, студент факультета вычислительной математики, организовывал сетевые атаки, заключающиеся в получении обманным путем доступа в сеть посредством имитации соединения. Таким образом он получил доступ к информации о счетах пользователей интернета и номерах некоторых кредитных карт и пин-кодов. Полученную информацию Гуляшов передавал Сорокиной за вознаграждение, которая использовала ее для хищения денежных средств.

Что такое фишинг, спуфинг и фарминг? Признаки какого явления усматриваются в деянии Гуляшова? (фишинга, спуфинга или фарминга). Квалифицируйте содеянное Гуляшовым и Сорокиной.

1. ГУВД Московской области было возбуждено уголовное дело по факту совершение неправомерного доступа в охраняемой законом компьютерной информации в кассовых аппаратах одного из индивидуальных предпринимателей г.Павловский Посад Лебедева. Следствие квалифицировало действие Лебедева по ч.2 ст.272 УК РФ, т.е. изменение информации в контрольно-кассовых аппаратах, при которых записанная в них сумма выручки за смену искусственно занижалась. Информация, содержащаяся в контрольно-кассовых аппаратах, признана следствием разновидностью компьютерной информации. Адвокат Лебедева настаивал на изменении квалификации.

Дайте юридическую оценку содеянного. Что следует понимать под компьтерной информацией?

9. Петров использовал доработанный сотовый телефон – «сканер», который позволял производить звонки за чужой счет. Всего в течение шести месяцев Петров таким образом «израсходовал» 15 тыс.рублей. Можно ли считать информацию, содержащуюся в сотовым телефоне, компьютерной информацией? Как соотносятся компьютерная информация и коммерческая тайна? Квалифицируйте содеянное Петровым.

1. Программист Мохов был признан судом виновным в деяниях, предусмотренных ч.3. ст.273 УК РФ и ч.1 ст.165 УК РФ. С ноября по апрель Мохов рассылал клиентам пяти городским Интернет-провайдерам «Троянские» программы и получал логины с паролями, которыми пользовался для доступа в Интернет. Всего было доказано наличие 12 подобных эпизодов, в течение которых Мохов пользовался услугами Интернета без оплаты.

Правильно ли суд квалифицировал содеянное? В каких случаях возможна квалификация по совокупности деяний, предусмотренных ст.272-274 УК РФ с иными составами преступлений? Что следует понимать под тяжкими последствиями, применительно к составу преступления, предусмотренного ст.273 УК РФ?

1. Панченко и Будин, работали в компьютерной форме, распространяли «Троянские» программы и получали доступ к паролям пользователей компьютеров. Следствие квалифицировало распространение вирусных программ по ч.1 ст.273 УК РФ, а доступ к чужим паролям по ч.1. ст.272 УК РФ.

Дайте анализ объективных и субъективных признаков данных составов преступлений. Решите вопрос о квалификации содеянного.

Контроль текущих знаний:

Задание 1: **Системный подход к решению проблем**

Ответ:

Системный анализ — это взаимосвязанное логико-математическое и комплексное рассмотрение всех вопросов, относящихся не только к замыслу, разработке, производству, эксплуатации и последующей ликвидации современных технических средств, но и к методам руководства всеми этими этапами с учетом социальных, политических, стратегических, психологических, правовых, географических, демографических, военных и других аспектов.

Понятие «система» появилось в Древней Греции 2000—2500 лет назад и первоначально означало: сочетание, организм, устройство, организация, строй, союз. Оно также выражало определенные акты деятельности и их результаты (нечто, поставленное вместе; нечто, приведенное в порядок).

Первоначально слово «система» было связано с формами социально-исторического бытия. Лишь позднее принцип порядка, идея упорядочивания переносятся на Вселенную.

Перенос значения слова с одного объекта на другой и вместе с тем превращение слова в обобщенное понятие совершаются поэтапно. Метафориза-

ция слова «система» была начата Демокритом (460—360 до н. э.), древнегреческим философом. Образование сложных тел из атомов он уподобляет образованию слов из слогов и слогов из букв. Сравнение неделимых форм (элементов с буквами) — один из первых этапов формирования научно-философского понятия, обладающего обобщенным универсальным значением.

Попытки разработать общие принципы системного подхода были предприняты врачом, философом и экономистом А.А. Богдановым (1873—1928) в работе «Всеобщая организационная наука (тектология)». Основная идея тектологии — признание необходимости подхода к любому явлению со стороны его системности.

То есть Богдановым было положено зарождение такого понятия, как системное мышление.

Системное мышление – метод, с помощью которого можно выделить определенные закономерности. Определенный смысл в ряду событий и явлений, чтобы лучше подготовится к будущему, и получить возможность оказать на него влияние. Таким образом человек, используя системное мышление, как метод познания окружающего мира и решения жизненных ситуаций получает инструмент управления своим будущим, то есть формирования будущего в желаемом человеком виде.

Одним из основных составляющих системного мышления является системный подход.

Системный подход – способ познания, основа ясного мышления и нормального взаимоотношения. Системный поход позволяет больше понимать и лучше видеть сложившуюся проблему, а, следовательно, позволяет лучше разобраться в том, что происходит, а затем предпринять действия, которые принесут более долговременный эффект.

То есть подход к решению проблем и проблемных ситуаций, называемый системным координально отличается от принятого и привычного для большинства традиционного мышления. Но люди живут с таким мышлением многие годы и довольны. Возникает вопрос зачем же нам нужен системный подход?

Задание 2: **Для чего нужен системный подход в области ИБ**

Ответ:

Системный подход нужен для того, чтобы:

1. Знать, как устроен мир (то есть воспринимать его как живую систему) и совершать гораздо меньше ошибок. Если человек с раннего детства будет знать элементарные основы системного подхода, то избежит в своей жизни системных ошибок. На практике же получается, особенно в России, что, начиная со школьной скамьи, ребенку прививают традиционный способ мышления. То есть не развивают логику и способность творчески мыслить, а учат действовать по шаблону, по уже знакомым цепочкам действий. Допустим, дают задачу с готовым алгоритмом решения и затем еще несколько за-

дач на тот же алгоритм, поэтому ребенок, встретив задачу, неподходящую под знакомый ему алгоритм не может ее решить.

2. Правильно формулировать свои цели и обеспечить их выполнение. Этот момент особенно важен для жизни каждого человека. Так как правильно и точно сформулированная цель – это уже половина успеха.

3. Правильно исследовать любые системы, быстро изучать их, то есть не тратить время на мелочи, но и не пропускать главное. То есть человек, смотрящий на объект, как систему, состоящую из множества частей, способен выявить в объекте наиболее важные для изучения аспекты, а, следовательно, сэкономить время на изучение объекта в целом.

4. Эффективно управлять системами. Здесь действует тот же принцип, который мы рассмотрели выше. Особенно это важно для человека, организующего работу нескольких специалистов.

5. Правильно создавать новые системы любой природы. Используя основные принципы моделирования систем в рамках системного подхода можно сравнительно быстро и качественно создать любую систему, начиная от какой-либо технической системы, заканчивая бизнесс-системой, то есть фирмой.

6. Резко увеличить качество своих решений и сократить время на процесс их принятия.

7. Уметь объединять знание многих наук. Как раз умение для принятия решения, использовать разнородные знания и есть системное мышление.

8. Не дать себя обмануть, когда объект необъективно расхваливают, рассматривая его только, с одной стороны. То есть если в магазине вам упорно пытаются продать какой-либо товар, объясняя удачность покупки его низкой привлекательной ценой, а сегодня еще и скидки 40 %, то нужно включить системное мышление и задуматься о других составляющих частях покупки, таких как качество, надежность и вообще нужен ли вам сейчас этот товар. Но это с бытовой точки зрения. Также сюда относят распознавание достоверной информации среди той, что нам предоставляют различные средства информации. Так как на одном канале информация может рассматриваться односторонне, а это в большинстве случаев так и происходит, таким образом являться недостоверной.

9. Научиться прогнозировать события. То есть возможность сопоставлять факты и делать соответствующие выводы.

В основе системного подхода лежат три основных процесса.

Анализ системы – изучение частей системы и связи между ними (выявление внутренних связей). А также связей между системой и внешним миром (выявление внешних связей).

Более сложный процесс это.

Синтез системы – соединение частей в единое целое на основе знаний, полученных при анализе.

И наиболее сложный процесс мышления это.

Творчество – создание нового, то есть синтез на основе анализа. Считается, что каждый человек способен к творчеству, но не каждый человек желает эти способности развивать.

То есть вот мы с вами рассмотрели зачем нужен системный подход, выявили его основные положительные моменты, но в начале лекции я говорила о том, что большинству людей традиционное мышление, не только привычнее, но нам его прививают с детства. Почему же, если системный подход так хорош, он так мало известен? Оказывается, на это есть свои причины.

Причины малоизвестности системного подхода:

1. Во-первых, до настоящего времени системный подход применяется главным образом в технике и в математике. Ограничивая его использование исключительно сферой академических наук.
2. Во-вторых, сама система нашего образования не поспевает за потоком открытий, в следствие своей громоздкости, то есть слишком медленно реагирует на появление новых идей. Школьные и университетские программы на несколько лет отстают от современности, и чтобы сократить разрыв потребуются годы. Это в некоторой степени связано и с бюрократичностью нашей системы образования, то есть для того чтобы новая программа обучения начала реализовываться на практике, необходимо ее детально описать, а затем апробировать, а затем утвердить во множестве инстанций. На это может потребоваться не только несколько месяцев, но и несколько лет. Пример: программа обучения на компьютерных дисциплинах.

Вывод: привычное мышление при изучении оказывается не эффективным, поскольку оно направлено на поиски простых цепочек причинно-следственных связей, протянутых в пространстве и времени, а не на выявление всей конкретной сложности сочетания всех взаимосвязанных факторов.

Задание 3: Понятие объекта в системном подходе в области ИБ

Ответ:

Основополагающим понятием системного подхода как метода решения проблем является понятие объекта.

Объект – это любой предмет, явление, процесс или состояние. Которое воспринимается нами как единое целое, характеризуется признаками и имеет определенное имя.

Объекты бывают активные и пассивные.

Активные объекты – объекты, которые могут изменять свое состояние и проявлять свое поведение, без воздействия со стороны других объектов. То есть они сами являются источниками воздействия (в большинстве случаев такие объекты называют субъектами).

Пассивные объекты – объекты, которые могут изменять свое состояние только под воздействием внешней среды. То есть они являются объектами, на которых направлено воздействие.

У каждого объекта есть свои признаки, благодаря которым он индивидуален, к таким признакам относят:

- Свойство об.

- Состояние об. в данный момент времени
- Поведение об.
- Действие об.
- Совокупность частей об.

Любой объект проявляет себя как система, то есть как совокупность взаимосвязанных элементов, а также средство для достижения целей.

То есть любой объект есть система, которая существует в определенной среде, называемой внешним миром, и, кроме того, в этом внешнем мире существуют и субъекты, которые могут самостоятельно воздействовать на объект.

При взаимодействии объекта и субъекта может возникнуть проблемная ситуация, кроме того, она может возникнуть, когда субъекта не удовлетворяет состояние или поведение объекта.

Взаимодействие субъекта и объекта можно разделить на два направления:

1. Практическая деятельность.
2. Познавательная деятельность.

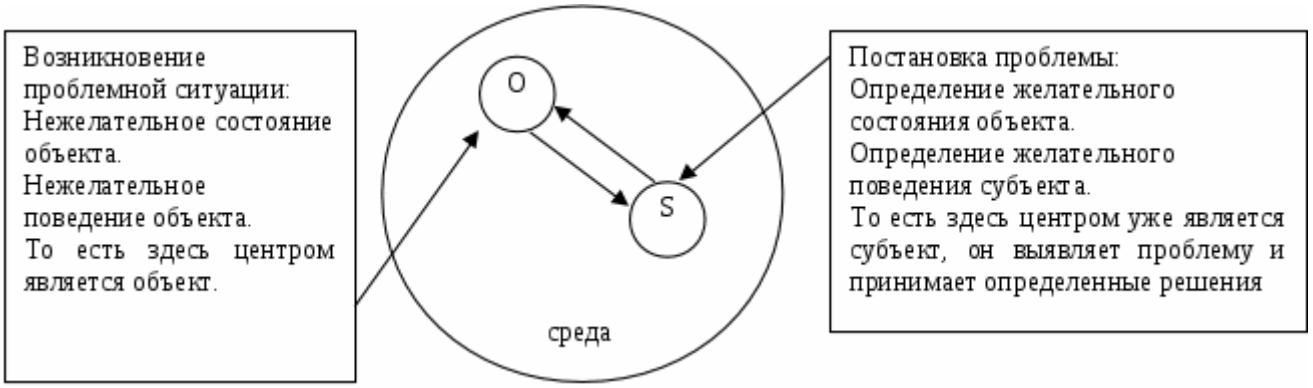
Практическая деятельность включает:

1. Целеполагание (постановка цели управления объектом).
2. Технология управления (методы и средства воздействия на объект, для приведения его к цели, поставленной субъектом).

Познавательная деятельность включает:

1. Изучение объекта путем анализа (выявление значимых параметров и компонентов, а также связей между ними) и синтеза (выявление правил построения объекта из отдельных компонентов).
2. Исследование динамики (поведения в тех или иных конкретных условиях) и разработка методов прогноза (предсказания реакции на различные воздействия).

Важным моментом системного подхода является проведение отчетливой границы между возникновением проблемной ситуации и связанной с ней проблемой. То есть у нас есть два понятия проблемная ситуация и проблема. Понятия близкие, но при использовании системного подхода абсолютно нетождественные. Сначала возникает проблемная ситуация, а уже из нее появляется сама проблема. Рассмотрим, как это происходит и в чем различие данных понятий. Мы обозначили, что у нас есть определенная среда, в которой сосуществуют объект и субъект.



Вывод: при системном подходе к деятельности под проблемной ситуацией имеется в виду то обстоятельство, что субъект не удовлетворен либо состоянием, в котором находится объект, либо его поведением. Однако, при этом субъекту еще не известно, какое состояние или поведение объекта его удовлетворит. Проблемная ситуация перерастает в проблему в том случае, когда каким-либо образом удается конкретизировать возникшую неопределенность и определить желаемое состояние или поведение объекта.

Задание 4: **Выделение определенной цели для решения четко сформулированной проблемы субъектом ИБ**

Ответ:

Цель – это то, к чему мы стремимся, что хотим получить в результате воздействия на объект. Цель может включать в себя несколько последовательных задач или подцелей, выполнение которых позволит прийти к конечной цели.

Цель -> Подцель1 -> Подцель2 -> … -> Подцель n -> Конечная цель.

Рассмотрим описанные выше выводы на конкретном примере. Допустим, вы субъект, у которого есть своя личная комната, которая в данном случаи будет являться объектом. Одним прекрасным днем вы зашли в свою комнату или же проснулись ранним утром и поняли, что вас в этой комнате что-то стало не устраивать. То есть возникла проблемная ситуация – вас не устраивать состояние объекта. Вы включаете мышление и, конкретизировав создавшеюся проблемную ситуацию, понимание, что вас не устраивают в данной комнате обои, они уже какие-то старые, да и цвет вам уже не нравится. То есть, сформулирована проблема и поставлена цель – нужно поклеить новые обои. А вот уже подцели на пути к конечной у каждого будут разные. …….. То есть конечная цель одна, а методы решения проблемы у каждого свои. А вообще в системном анализе существуют разработанные научные методы решения проблем.

Задание 5: **Методы решения проблем**

Ответ:

1) Метод проб и ошибок.

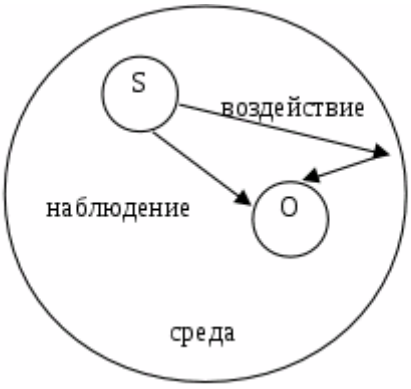
Суть метода: на объект оказывается некоторое воздействие и происходит наблюдение за его состоянием или поведением, с точки зрения приближаемся мы к цели или нет.

Недостатки метода:

1. Метод может привести к разрушению объекта из-за недопустимого воздействия.
2. В тех случаях, когда цель все же достигается, нет уверенности, что это осуществляется наилучшим образом. То есть может быть, при выборе другого воздействия на объект процесс протекал бы быстрее или качественнее.
3. При управлении этим методом довольно трудно обобщить правила воздействия на объект, чтобы использовать опыт управления при решении других проблем с этим же объектом или аналогичных проблем с другими объектами. То есть вы выбрали какой-то способ воздействия на объект, он оказался удачным и цель достигнута. Но так как вы сделали выбор на обум, не факт, что при повторном воздействии на этот же объект, а уж тем более на другие объекты этот метод воздействия будет также удачен.

2) Метод воздействия на окружающую среду.

Суть метода: надежда на достижение целей основана на эффекте влияния среды на состояние и поведение объекта.



То есть воздействие не напрямую на объект, а влияние на его поведение и состояние через внешнюю среду.

Недостатки метода: при воздействии на окружающую среду меньше шансы достижения цели, поскольку состояние объекта зависит от воздействий косвенным и сложным образом

Достоинства метода: по сравнению с прямым воздействием на объект, здесь можно рассчитывать на повышение безопасности, а также эффективности воздействия.

Пример положительного воздействия: поместить подростка в положительную компанию.

Пример, когда такое воздействие не приносит результатов: если надолго оставить автомобиль под воздействием открытого пространства, он начнет ржаветь, и если после этого его переставить в гараж, легче не станет.

3) Описание модели объекта (системы)

Суть метода: системный подход к решению проблем заключается в том, что решение проблем начинается с познания объекта (системы) для осознанных практических действий с предсказуемыми последствиями. Для решения возникшей проблемы нужно построить реальную модель объекта. Она должна быть по возможности простая, но в то же время не исключать ни од-

ной составляющей части связей и функциональности объекта. Это необходимо для того, чтобы предсказать нежелательные явления при взаимодействии с реальным объектом. То есть необходимо провести моделирование, исследовать упрощенную копию, схему, образ, заменитель объекта (модель) с учетом среды, в которой находится объект.

Подготовка ответов на задания самостоятельной работы

Методика оценки (анализа) угроз безопасности информации в рамках системного анализа

Моделирование угроз безопасности информации - позволяет проводить упреждающую оценку, анализировать и определять приоритеты в работе по устранению угроз, обеспечивая эффективное распределение ресурсов. Ключом к моделированию угроз является определение того, где следует прилагать наибольшие усилия для обеспечения безопасности системы. Эта переменная изменяется по мере того, как добавляются, удаляются или модернизируются информационные системы, приложения, а также изменяются пользовательские требования.

Моделирование угроз - это итеративный процесс, который состоит из определения активов предприятия, определения того, что каждая информационная система делает с этими активами, создания профиля безопасности для каждой ИС, определения потенциальных угроз, установления приоритетов. Моделирование угроз может помочь обеспечить соответствие защиты меняющимся угрозам. В противном случае новые угрозы могут оставаться незащищенными, оставляя системы и данные уязвимыми.

Что определяет методика оценки (анализа) угроз безопасности информации?

Методика определяет порядок и содержание работ по определению угроз безопасности информации, реализация (возникновение) которых возможна в информационных системах, автоматизированных системах управления, информационно-телекоммуникационных сетях, информационно-телекоммуникационных инфраструктурах центров обработки данных и облачных инфраструктурах , а также по разработке моделей угроз безопасности информации систем и сетей.

Когда применяется методика?

Методика применяется для определения угроз безопасности информации, реализация (возникновение) которых возможна в системах и сетях, отнесенных к государственным и муниципальным информационным системам, информа-

ционным системам персональных данных, значимым объектам критической информационной инфраструктуры Российской Федерации, информационным системам управления производством, используемым организациями оборонно-промышленного комплекса автоматизированным системам управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объекта, объектах, представляющих повышенную опасность для жизни и здоровья людей и окружающей природной среде.
В иных случаях решение о применении методики принимается обладателями или операторами систем и сетей.

По сути, данная методика необходима для большинства информационных систем и сетей.

Основные задачи оценки (анализа) угроз безопасности информации
• определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации;
• инвентаризация систем и сетей и определение возможных объектов воздействия угроз безопасности информации;
• определение источников угроз безопасности информации и оценка возможностей нарушителей по реализации угроз безопасности информации;
• оценка способов реализации (возникновения) угроз безопасности информации;
• оценка возможности реализации (возникновения) угроз безопасности информации и определение актуальности угроз безопасности информации;
• оценка сценариев реализации угроз безопасности информации в системах и сетях.

Ранее для определения потенциальных угроз безопасности информации использовались следующие методики:
• Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (2016 года);
• Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры (20016 года).

Новая методика ФСТЭК по оценке угроз безопасности информации актуализирована и более универсальна.

Общая схема проведения моделирования угроз:
Этап 1. Определение негативных последствий от угроз безопасности информации.
- Анализ документации систем и сетей, и иных исходных данных;
- Определение негативных последствий от реализации угроз.

Этап 2. Определение объектов воздействия угроз безопасности информации.

- Анализ документации систем и сетей, и иных исходных данных;
- Инвентаризация систем и сетей;
- Определение групп информационных ресурсов и компонентов систем и сетей.

Этап 3. Оценка возможности реализации угроз и их актуальности.

- Определение источников угроз;
- Оценка способов реализации угроз;
- Оценка актуальности угроз.

1. Исходными данными для определения негативных последствий, объектов воздействия и источников угроз являются:

- Банк данных угроз безопасности ФСТЭК;
- Модели угроз безопасности ФСТЭК;
- Отраслевые модели угроз;
- Нормативно-правовые акты;
- Результаты анализа рисков;
- Документация на системы и сети;
- Базы знаний (ATT&CK, OWASP, CAPEC и др.);
- Технологические, производственные карты или иные документы, содержащие описание основных бизнес-процессов;
- Договоры, соглашения или иные документы, содержащие условия использования информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры поставщика услуг.

2. На основе анализа исходных данных определяются событие или группа событий, наступление которых в результате реализации (возникновения) угроз безопасности информации может привести к:

- Нарушению прав граждан;
- Возникновению ущерба в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности государства;
- Возникновению финансовых, производственных, репутационных или иных рисков (видов ущерба) для обладателя информации, оператора.

3. Далее должны быть определены информационные ресурсы и компоненты систем и сетей, несанкционированный доступ к которым или воздействие на которые в ходе реализации (возникновения) угроз безопасности информации может привести к негативным последствиям – объ-

екты воздействия:

- информация (данные), содержащаяся в системах и сетях (в том числе защищаемая информация, персональные данные, информация о конфигурации систем и сетей, данные телеметрии, сведения о событиях безопасности и др.)
- программно-аппаратные средства обработки и хранения информации (в том числе автоматизированные рабочие места, серверы, включая промышленные, средства отображения информации, программируемые логические контроллеры, производственное, технологическое оборудование (исполнительные устройства));
- программные средства (в том числе системное и прикладное программное обеспечение, включая серверы приложений, веб-приложений, системы управления базами данных, системы виртуализации);
- машинные носители информации, содержащие как защищаемую информацию, так и аутентификационную информацию;
- телекоммуникационное оборудование (в том числе программное обеспечение для управления телекоммуникационным оборудованием);
- средства защиты информации (в том числе программное обеспечение для централизованного администрирования средств защиты информации);
- привилегированные и непривилегированные пользователи систем и сетей, а также интерфейсы взаимодействия с ними;
- обеспечивающие системы.

Совокупность объектов воздействия и их интерфейсов определяет границы процесса оценки угроз безопасности информации и разработки модели угроз безопасности информации.

К основным информационным ресурсам и компонентам систем и сетей могут относиться системы хранения данных (базы данных), системы управления базами данных, веб-сайт, почтовый сервер, почтовый клиент, автоматизированное рабочее место пользователя, система управления и администрирования, контроллер домена, сетевые службы, проводные и беспроводные каналы передачи данных, телекоммуникационное оборудование и т.д.

4. Для определенных информационных ресурсов и компонентов систем и сетей должны быть определены виды воздействия на них, которые могут привести к негативным последствиям. Основными видами таких воздействий являются:

- утечка (перехват) конфиденциальной информации или отдельных данных (нарушение конфиденциальности)
- несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным;
- отказ в обслуживании компонентов (нарушение доступности);

- несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности);
- несанкционированное использование вычислительных ресурсов систем и сетей в интересах решения несвойственных им задач;
- нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации.

5. На основе анализа исходных данных, а также результатов оценки возможных целей реализации нарушителями угроз безопасности информации определяются виды нарушителей, актуальных для систем и сетей. Основными видами нарушителей, подлежащих оценке, являются:
- специальные службы иностранных государств;
- террористические, экстремистские группировки;
- преступные группы (криминальные структуры);
- отдельные физические лица (хакеры);
- конкурирующие организации;
- разработчики программных, программно-аппаратных средств;
- лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем;
- поставщики услуг связи, вычислительных услуг;
- лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ;
- лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.); авторизованные пользователи систем и сетей;
- системные администраторы и администраторы безопасности;
- бывшие (уволенные) работники (пользователи).

Указанные виды нарушителей могут быть дополнены иными нарушителями с учетом особенностей области деятельности, в которой функционируют системы и сети. Для одной системы и сети актуальными могут являться нарушители нескольких видов. Нарушители признаются актуальными для систем и сетей, когда возможные цели реализации ими угроз безопасности информации могут привести к определенным для систем и сетей негативным последствиям и соответствующим рискам (видам ущерба).
Нарушители имеют разные уровни компетентности, оснащенности ресурсами и мотивации для реализации угроз безопасности информации. Совокупность данных характеристик определяет уровень возможностей нарушителей по реализации угроз безопасности информации.
В зависимости от уровня возможностей нарушители подразделяются на нарушителей, обладающих:
- базовыми возможностями по реализации угроз безопасности информации (Н1);

- базовыми повышенными возможностями по реализации угроз безопасности информации (Н2);
- средними возможностями по реализации угроз безопасности информации (Н3);
- высокими возможностями по реализации угроз безопасности информации (Н4).

Для одной системы или сети актуальными могут являться нарушители, имеющие разные уровни возможностей.

По результатам определения источников угроз безопасности информации должны быть определены:
а) виды актуальных нарушителей и возможные цели реализации ими угроз безопасности информации, а также их возможности;
б) категории актуальных нарушителей, которые могут реализовывать угрозы безопасности информации, в том числе непреднамеренные угрозы.

6. На основе анализа исходных данных, а также возможностей нарушителей определяются способы реализации (возникновения) угроз безопасности информации, актуальные для систем и сетей.

Основными способами реализации (возникновения) угроз безопасности информации являются:
- использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей);
- внедрение вредоносного программного обеспечения;
- использование не декларированных возможностей программного обеспечения и (или) программно-аппаратных средств;
- установка программных и (или) программно-аппаратных закладок в программное обеспечение и (или) программно-аппаратные средства;
- формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных;
- перехват (измерение) побочных электромагнитных излучений и наводок (других физических полей) для доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации;
- инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации;
- нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам (в том числе администрированию, обслуживанию);
- ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств.

Указанные способы реализации (возникновения) угроз безопасности информации могут быть дополнены иными способами с учетом особенностей архитектуры и условий функционирования систем и сетей.

Условием, позволяющим нарушителям использовать способы реализации угроз безопасности информации, является наличие у них возможности доступа к следующим типам интерфейсов объектов воздействия:
- внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными (взаимодействующими) системами или сетями (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др.);
- внутренние сетевые интерфейсы, обеспечивающие взаимодействие (в том числе через промежуточные компоненты) с компонентами систем и сетей, имеющими внешние сетевые интерфейсы (проводные, беспроводные);
- интерфейсы для пользователей (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др.);
- интерфейсы для использования съемных машинных носителей информации и периферийного оборудования;
- интерфейсы для установки, настройки, испытаний, пусконаладочных работ (в том числе администрирования, управления, обслуживания) обеспечения функционирования компонентов систем и сетей;
- возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей.

По результатам оценки возможных способов реализации угроз безопасности информации должны быть определены:
а) виды и категории нарушителей, которые имеют возможность использования актуальных способов;
б) актуальные способы реализации угроз безопасности информации и типы интерфейсов объектов воздействия, за счет которых они могут быть реализованы.

7. На основе анализа исходных данных определяются возможные для систем и сетей угрозы безопасности информации, к которым относятся осуществляемые нарушителем воздействия на информационные ресурсы и компоненты систем и сетей (объекты воздействия), в результате которых возможно нарушение безопасности информации и (или) нарушение или прекращение функционирования систем и сетей.
Угроза безопасности информации возможна, если имеются нарушитель или иной источник угрозы, объект, на который осуществляются воздействия, способы реализации угрозы безопасности информации, а реализация угрозы может привести к негативным последствиям.
Актуальность возможных угроз безопасности информации определяется

наличием сценариев их реализации.

Сценарии реализации угроз безопасности информации должны быть определены для соответствующих способов реализации угроз безопасности информации, определенных в соответствии с настоящей Методикой, и применительно к объектам воздействия и видам воздействия на них.

Определение сценариев предусматривает установление последовательности возможных тактик и соответствующих им техник, применение которых возможно актуальным нарушителем с соответствующим уровнем возможностей, а также доступности интерфейсов для использования соответствующих способов реализации угроз безопасности информации.

На этапе создания систем и сетей должен быть определен хотя бы один сценарий каждого способа реализации возможной угрозы безопасности информации. Сценарий определяется для каждого актуального нарушителя и их уровней возможностей.

На этапе эксплуатации определение сценариев реализации угрозы включает:
- анализ исходных данных на систему или сеть, предусматривающий в том числе анализ документации, модели угроз безопасности информации, применяемых средств защиты информации, и определение планируемых к применению автоматизированных средств;
- проведение инвентаризации информационных систем и сетей и определение объектов воздействия и их интерфейсов;
- определение внешних интерфейсов, которые могут быть задействованы при реализации угроз безопасности информации;
- определение внутренних интерфейсов, которые могут быть задействованы при реализации угроз безопасности информации;
- выявление уязвимостей объектов воздействия, а также компонентов систем и сетей, имеющих внешние интерфейсы, с которыми посредством внутренних интерфейсов взаимодействуют объекты воздействия;
- проведение тестирования на проникновение, подтверждающего возможность использования выявленных уязвимостей или выявления новых сценариев реализации угрозы безопасности информации;
- поиск последовательности тактик и техник, применение которых может привести к реализации угрозы безопасности информации, исходя из уровня возможностей актуальных нарушителей, а также результатов инвентаризации, анализа уязвимостей и тестирования на проникновение;
- составление сценариев реализации угрозы безопасности информации применительно к объектам и видам воздействия, а также способам реализации угроз безопасности информации.

Критерии оценки текущих знаний.

Шкала оценивания:

5 баллов («отлично») – Обучающийся смог показать прочные знания основных положений фактического материала, умение самостоятельно решать конкретные практические задачи повышенной сложности, свободно использовать справочную литературу, делать обоснованные выводы из результатов анализа конкретных проблемных ситуаций.

4 балла («хорошо») – Обучающийся смог показать прочные знания основных положений фактического материала, умение самостоятельно решать конкретные практические задачи, предусмотренные рабочей программой, ориентироваться в рекомендованной справочной литературе, умеет правильно оценить полученные результаты анализа конкретных проблемных ситуаций.

3 балла («удовлетворительно») – Обучающийся смог показать знание основных положений фактического материала, умение получить с помощью преподавателя правильное решение конкретной практической задачи из числа предусмотренных рабочей программой, Обучающийся знаком с рекомендованной справочной литературой;

2 балла («неудовлетворительно») – при ответе обучающегося выявились существенные пробелы в знаниях основных положений фактического материала, неумение с помощью преподавателя получить правильное решение конкретной практической задачи из числа предусмотренных рабочей программой.

Приложение 2
Методические указания для обучающихся по освоению дисциплины (модуля)

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И УПРАВЛЯЮЩИХ СИСТЕМ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ) ТЕОРИЯ СИСТЕМ И СИСТЕМНЫЙ АНАЛИЗ

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 «Теория систем и системный анализ» является совершенствование подготовки и повышение квалификации кадров в сфере информационно-технологических дисциплин для преподавательской деятельности и применения современных образовательных технологий; обучение методам *познания, анализа, структурирования моделей процессов и объектов, а также методологии формализации задачи принятия решений* для **достижения** определенной **цели**, для которой создается (выделяется) некоторая *искусственная система*; а также умение применять эти знания при решении конкретных задач.

Задачами дисциплины:

- Формирование понятия о системном подходе, системном анализе.
- Обучение построению модели системы.
- Изучение способов классификации систем.
- Освоение основных методологических принципов анализа систем

2. Указания по проведению практических (семинарских) занятий:

Тема 2. Системы и закономерности их функционирования и развития.

Практическое занятие 1.

Вид практического занятия**:** *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

План занятия:

Цель занятия: рассмотреть основные положения системного анализа; освоить технологию формализации задачи для построения модели системы.

Основные положения темы занятия:

1. Системная парадигма. Аналитический и программно-целевой метод.
2. Процедуры управления системами: планирование; контроль; завершение.

Вопросы для обсуждения

1. Различные подходы к определению системы
2. Установление границ системы: система в целом, полная система и подсистемы.
3. Задачи и цели системы. Классификация целей.
4. Структура системы. Состояния и потоки.

5. Алгоритмичность системы. Свойства системы.
   Продолжительность занятия **– *4 ч.***

Тема 3. Классификация систем.

Практическое занятие 2.

Вид практического занятия**:** *подготовка доклада.*
Образовательные технологии: *беседа.*

План занятия:

Цель занятия: Исследование подходов к выделению типа системы; выделению характерных признаков систем.

Основные положения темы занятия:

1. Физические и абстрактные системы; естественные и искусственные; статические и динамические.
2. Дискретные, непрерывные и импульсные системы.
3. Технические, организационные и информационные системы.

Вопросы для обсуждения

1. Классификация систем по С.Биру и К.Боулдингу.
2. Классификация целей системы.
3. Меры эффективности – критерии достижения целей.
4. Примеры применения системного подхода к изучению систем различной природы.

Продолжительность занятия **– *4 ч.***

Тема 5.Свойства системы.

Практическое занятие 3.

Вид практического занятия**:** *подготовка доклада.*
Образовательные технологии: *практическая подготовка в группах.*

Цель занятия: Научиться выделять характерные свойства системы и применять методы оценки меры сложности системы.

Основные положения темы занятия:

1. Структурные свойства: иерархическая упорядоченность; централизация, вертикальная целостность и горизонтальная обособленность.
2. Динамические свойства: систематизация, изоляция, рост, стабильность, инерция.
3. Свойства, характеризующие управляемость системой: нечеткость информации, многокритериальность описания, неоднозначность оптимизации.

4. Методы экспертных оценок.

Вопросы для обсуждения

1. Многоаспектность понятия сложности: структурная, вычислительная, динамическая сложность системы
2. Основные принципы оценки сложности системы
3. Классификация задач по сложности
4. Машина Тьюринга
5. Временн*ая* функция сложности

Продолжительность занятия **– *4 ч.***

Тема 6.Системное моделирование.

Практическое занятие 4.

Вид практического занятия**:** *подготовка доклада.*

Образовательные технологии: *беседа*

План занятия:

Цель занятия: рассмотреть проблемы анализа и синтеза; применение математического аппарата исследования операций для построения типичных моделей экономических и организационных систем.

Основные положения темы занятия:

1. Алгоритмы анализа и синтеза.
2. Внешняя среда и внутренние ограничения.
3. Задачи планирования производства, транспортная и составления расписаний.
4. Принципы отбора, используемые при моделировании на разных уровнях организации систем.
5. Механизмы поддержания равновесия в системах.
6. Роль обратной связи в задачах управления системой.
7. Модели без управления.

Вопросы для обсуждения

1. Типы ограничений в задачах системного моделирования.
2. Физические и критериальные ограничения.
3. Моделирование поведения динамических систем.
4. Кибернетические системы.
5. Оптимизационные системы.

6. Взаимосвязь модели структуры, модели программы и модели поведения.

Продолжительность занятия – ***4 ч.***

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.	Системы и закономерности их функционирования и развития.	***Подготовка докладов и презентаций по темам:*** Различные подходы к определению системы Установление границ системы: система в целом, полная система и подсистемы. Задачи и цели системы. Классификация целей. Классификация компьютерных систем, подлежащих защите в зависимости от обрабатываемой информации и функционального назначения. Классификация СВТ по уровню защищённости от НСД к информации. Перечень показателей защищённости СВТ и совокупности описывающих их требований. Характеристика классов защищённости СВТ от НСД к информации. Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников.
2.	Классификация систем.	***Подготовка докладов и презентаций по темам:*** Классификация систем по С.Биру и К.Боулдингу.

		Классификация целей системы. Меры эффективности – критерии достижения целей.
3	Свойства системы	***Подготовка докладов и презентаций по темам:*** Основные принципы оценки сложности системы Классификация задач по сложности Машина Тьюринга Классификация компьютерных систем, подлежащих защите в зависимости от обрабатываемой информации и функционального назначения. Классификация СВТ по уровню защищённости от НСД к информации. Перечень показателей защищённости СВТ и совокупности описывающих их требований. Характеристика классов защищённости СВТ от НСД к информации. Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников
4	Системное моделирование	***Подготовка докладов и презентаций по темам:*** Моделирование поведения динамических систем. Кибернетические системы. Оптимизационные системы. Перечень основных документов ФСТЭК России по вопросам защиты информации. Система разграничения доступа (СРД) и её функции. Средства для СРД. Реализация СРД. Построение модели нарушителя безопасности АС. Уровни возможностей, предоставляемые нарушителям штатными средствами АС и СВТ. Базовая модель угроз ИСПДн.

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.Теория систем и системный анализ : учебник / С.И. Маторин, А.Г. Жихарев, О.А. Зимовец, М.Ф. Тубольцев, А.А. Кондратенко; под ред. С. И. Маторин. - Москва|Берлин : Директмедиа Паблишинг, 2020. - 509 с. : 509. - ISBN 978-5-4499-0675-5.
URL: http://biblioclub.ru/index.php?page=book&id=574641

2.Самойленко, А. П. Информационные технологии статистической обработки данных : учебное пособие / А.П. Самойленко, О.А. Усенко; Министерство образования и науки Российской Федерации; Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет»; Инженерно-технологическая академия. - Ростов-на-Дону|Таганрог : Издательство Южного федерального университета, 2017. - 127 с. : ил. - ISBN 978-5-9275-2521-8. - Электронная программа (визуальная).

Электронные данные : электронные.
URL: http://biblioclub.ru/index.php?page=book&id=500042

Дополнительная литература:

3.Бродовская, Е. В.Большие данные в исследовании политических процессов : учебное пособие / Е.В. Бродовская, А.Ю. Домбровская; Министерство науки и высшего образования Российской Федерации; Московский педагогический государственный университет. - Москва : МПГУ, 2018. - 88 с. : схем., табл., ил. - ISBN 978-5-4263-0712-4. - Текст (визуальный) : непосредственный.
URL: http://biblioclub.ru/index.php?page=book&id=563578
4.Аврунев, О. Е.Модели баз данных : учебное пособие / О.Е. Аврунев, В.М. Стасышин; Новосибирский государственный технический университет. - Новосибирск : Новосибирский государственный технический университет, 2018. - 124 с. : ил., табл. - ISBN 978-5-7782-3749-0.
URL: http://biblioclub.ru/index.php?page=book&id=575324
5.Голиков А. М. Тестирование и диагностика в инфокоммуникационных системах и сетях: курс лекций, компьютерные лабораторные работы и практикум, задание на самостоятельную работу; учебное пособие / А.М. Голиков. - Томск: ТУСУР, 2016. -436 с. - (Учебная литература для вузов).
URL: http://biblioclub.ru/index.php?page=book&id=480803

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).