

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Пекаревский Борис Владимирович
Должность: Проректор по учебной и методической работе
Дата подписания: 23.11.2023 13:34:42
Уникальный программный ключ:
3b89716a1076b80b2c167df0f27c09d01782ba84



МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Санкт-Петербургский государственный технологический институт
(технический университет)»

УТВЕРЖДАЮ
Проректор по учебной
и методической работе
_____ Б.В.Пекаревский
«24» мая 2021 г.

Рабочая программа дисциплины
СОВРЕМЕННЫЕ КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ В НАУКЕ И ЗАЩИТА
ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

Направление подготовки
27.04.03 Системный анализ и управление
Направленность программы магистратуры
«Системный анализ и управление в организационных системах»

Квалификация

Магистр

Форма обучения

Заочная

Факультет **информационных технологий и управления**
Кафедра **системного анализа и информационных технологий**

Санкт-Петербург

2021

Б1.О.04

ЛИСТ СОГЛАСОВАНИЯ

Должность разработчика	Подпись	Ученое звание, инициалы, фамилия
Доцент		доцент И.В. Ананченко

Рабочая программа дисциплины «Современные компьютерные технологии в науке и защита интеллектуальной собственности» обсуждена на заседании кафедры системного анализа и информационных технологий

протокол от «28» апреля 2021 № 7

Заведующий кафедрой,
профессор, д.т.н.

А.А. Мусаев

Одобрено учебно-методической комиссией факультета информационных технологий и управления

протокол от «19 » мая 2021 № 8

Председатель,
доцент, к.т.н.

В.В. Куркина

СОГЛАСОВАНО

Руководитель направления подготовки «Системный анализ и управление»		Д.А. Краснобородько
Директор библиотеки		Т.Н. Старостенко
Начальник методического отдела учебно-методического управления		Т.И. Богданова
Начальник учебно-методического управления		С.Н. Денисенко

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы	04
2. Место дисциплины в структуре образовательной программы.....	06
3. Объем дисциплины	06
4. Содержание дисциплины	
4.1. Разделы дисциплины и виды занятий.....	07
4.2. Занятия лекционного типа.....	08
4.3. Занятия семинарского типа.....	08
4.3.1. Семинары, практические занятия	08
4.4. Самостоятельная работа обучающихся.....	09
5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине	11
6. Фонд оценочных средств для проведения промежуточной аттестации.....	12
7. Перечень учебных изданий, необходимых для освоения дисциплины	12
8. Перечень электронных образовательных ресурсов, необходимых для освоения дисциплины.....	13
9. Методические указания для обучающихся по освоению дисциплины.....	13
10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине	
10.1. Информационные технологии.....	13
10.2. Программное обеспечение.....	14
10.3. Базы данных и информационные справочные системы.....	14
11. Материально-техническое обеспечение освоения дисциплины в ходе реализации образовательной программы	14
12. Особенности освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья	14
Приложения: 1. Фонд оценочных средств для проведения промежуточной аттестации.	

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

В результате освоения образовательной программы магистратуры обучающийся должен овладеть следующими результатами обучения по дисциплине:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения (дескрипторы)
<p>ОПК-3 Способен решать задачи системного анализа и управления в технических системах на базе последних достижений науки и техники</p>	<p>ОПК-3.1 Использование современных компьютерных технологий в задачах системного анализа</p>	<p>Знать: - современные компьютерные средства для решения задач системного анализа (ЗН-1). Уметь: - применять современные компьютерные средства для решения задач системного анализа (У-1). Владеть: - методами использования компьютерных технологий для решения прикладных научно-технических задач, в том числе системного анализа. (Н-1).</p>
	<p>ОПК-3.2 Исследование современных систем управления в технических системах</p>	<p>Знать: - методы создания сложных комплексов с использованием CASE-средств; знать, как контролировать качество разрабатываемых систем управления (ЗН-2). Уметь: - составлять модель по словесному описанию, настраивать модель, представлять модель в алгоритмическом и математическом виде; творчески использовать инструменты подготовки и принятия решений для системного анализа объектов химической технологии на основе лицензионных программных комплексов (У-2). Владеть: - навыками использования инструментов для подготовки и принятия решений для системного анализа объектов химической технологии на основе лицензионных программных комплексов (Н-2).</p>

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения (дескрипторы)
ОПК-5 Способен решать задачи в области развития науки, техники и технологии, применяя современные методы системного анализа и управления с учетом нормативно-правового регулирования в сфере интеллектуальной собственности	ОПК-5.1 Использование современных компьютерных технологий в задачах системного анализа	Знать: - методы и способы формализации объектов, процессов, явлений и реализации их на компьютере и способами представления информации о моделируемых объектах и их свойств в компьютере (ЗН-3). Уметь: - использовать прикладные системы ограничения доступа к научно-технической информации; выполнять поиск научной и научно-технической информации в компьютерных сетях и специализированных базах данных (У-3). Владеть: - навыками обеспечения информационной безопасности и защиты компьютеров и компьютерных сетей (Н-3).
	ОПК-5.2 Применение современных программных средств с учетом норм регулирования интеллектуальной собственности	Знать: - принципы применения современных программных средств с учетом норм регулирования интеллектуальной собственности (ЗН-4). Уметь: - внедрять методы применения современных программных средств с учетом норм регулирования интеллектуальной собственности (У-4). Владеть: - методами анализа применения современных программных средств с учетом норм регулирования интеллектуальной собственности (Н-4).

2. Место дисциплины в структуре образовательной программы.

Дисциплина относится к обязательной части (Б1.О.04), и изучается на 2 курсе.

В методическом плане дисциплина опирается на элементы компетенций, сформированные при изучении дисциплин «Математическое моделирование, функциональный анализ» и «Модели и методы построения систем управления технологическими процессами». Полученные в процессе изучения дисциплины «Современные компьютерные технологии в науке и защита интеллектуальной собственности» знания, умения и навыки могут быть использованы при выполнении научно-исследовательской работы, прохождении преддипломной практики, а также при выполнении выпускной квалификационной работы (магистерской диссертации).

3. Объем дисциплины.

Вид учебной работы	Всего, ЗЕ/акад. часов
Общая трудоемкость дисциплины (зачетных единиц/ академических часов)	4/144
Контактная работа с преподавателем:	26
занятия лекционного типа	6
занятия семинарского типа, в т.ч.	16
семинары, практические занятия (в том числе практическая подготовка)	16
лабораторные работы	
курсовое проектирование (КР или КП)	4
КСР	-
другие виды контактной работы	–
Самостоятельная работа	114
Форма текущего контроля (Кр, реферат, РГР, эссе)	Кр(2)
Форма промежуточной аттестации (КР, КП, зачет, экзамен)	Зачет(4), КР

4. Содержание дисциплины.

4.1. Разделы дисциплины и виды занятий.

№ п/п	Наименование раздела дисциплины	Занятия лекционного типа, акад. часы	Занятия семинарского типа, акад. часы		Самостоятельная работа, акад. часы	Формируемые компетенции	Формируемые индикаторы
			Семинары и/или практические занятия	Лабораторные работы			
1	Использование программных и аппаратных ключей серии для защиты программного обеспечения	1	2		14	ОПК-3	ОПК-3.1 ОПК-3.2
2	Использование аппаратных ключей для шифрования информации и работы с ЭЦП	1	2		20	ОПК-3	ОПК-3.1 ОПК-3.2
3	Развертывание и администрирование защищенных виртуальных частных сетей (на примере ПО VipNet)	1	2		20	ОПК-3	ОПК-3.1 ОПК-3.2
4	Обзор и анализ существующих компьютерных систем имитационного моделирования.	1	2		20	ОПК-5	ОПК-5.1 ОПК-5.2
5	CASE-технологии. Развитие методологии проектирования. Создание компьютерной модели исследуемого объекта управления.	1	4		20	ОПК-5	ОПК-5.1 ОПК-5.2
6	Обработка данных эксперимента, визуализация данных, создание компьютерной презентации.	1	4		20	ОПК-5	ОПК-5.1 ОПК-5.2

4.2. Занятия лекционного типа.

№ раздела дисциплины	Наименование темы и краткое содержание занятия	Объем, акад. часы	Инновационная форма
1	Использование программных и аппаратных ключей серии HASP HL и HASP SL для защиты программного обеспечения	0,5	Слайд-презентация
1	Использование программных и аппаратных ключей серии GUARDANT для защиты программного обеспечения	0,5	Слайд-презентация
2	Использование ключей серий eToken и ruToken для шифрования информации и ЭЦП	1	Слайд-презентация
3	Развертывание и администрирование защищенных виртуальных частных сетей (на примере ПО VipNet)	1	Слайд-презентация
4,5	Обзор и анализ существующих компьютерных систем имитационного моделирования.	2	Слайд-презентация
6	Обработка данных эксперимента, визуализация данных, создание компьютерной презентации.	1	Слайд-презентация

4.3. Занятия семинарского типа.

4.3.1. Семинары, практические занятия.

№ раздела дисциплины	Наименование темы и краткое содержание занятия	Объем, акад. часы	Инновационная форма
1	Использование программных ключей серии HASP HL и HASP SL для защиты программного обеспечения. GUARDANT - использование программных (GUARDANT SP) и аппаратных ключей серии для защиты программного обеспечения	2	групповая дискуссия
2	Использование ключей серий eToken и ruToken для шифрования информации и ЭЦП	2	групповая дискуссия
3	Развертывание и администрирование защищенных виртуальных частных сетей	2	групповая дискуссия
4	CASE-технологии. Развитие методологии проектирования. Создание компьютерной модели исследуемого объекта управления.	2	групповая дискуссия
5,6	Обработка данных эксперимента, визуализация данных, создание компьютерной презентации.	8	групповая дискуссия

4.4. Самостоятельная работа обучающихся.

№ раздела дисциплины	Перечень вопросов для самостоятельного изучения	Объем, акад. часы	Форма контроля
1	Защита программного обеспечения с помощью защиты навесного типа с использованием аппаратного ключа защиты серии HASP <ul style="list-style-type: none"> • представители ключей серии HASP HL, • использование HASP Envelope, • модели лицензирования ПО. 	2	Устный опрос № 1
1	Защита программного обеспечения с помощью защиты встраиваемого типа с использованием аппаратного ключа защиты серии HASP <ul style="list-style-type: none"> • подключение библиотек защиты HASP на уровне исходного кода, особенности встраиваемой защиты для выбранного языка программирования.	2	Устный опрос № 1
1	Защита программного обеспечения (библиотечных dll модулей) с помощью защиты встраиваемого типа с использованием аппаратного ключа защиты серии HASP <ul style="list-style-type: none"> • структура защищаемых dll библиотек, • анализ схемы защиты dll, особенности модели лицензирования	4	Устный опрос № 1
1	Защита исполняемых exe файлов с помощью навесной защиты HASP. Цель работы приобретение практических навыков работы с HASP ключами и программным обеспечением HASP SRM Vendor Suite. Защита исполняемых exe файлов.	6	Контрольная работа №1
2	Организация встроенной защиты программы, написанной на Delphi с помощью SENTINEL HASP API. Защита DLL библиотек с помощью Sentinel HASP. разработать программу средствами Delphi, использующую динамически подключаемую библиотеку DLL, защищенную с помощью Sentinel HASP.	4	Устный опрос № 2
2	Защита программного обеспечения с помощью защиты навесного типа с использованием аппаратного ключа защиты серии CUARDANT <ul style="list-style-type: none"> • установка инструментария разработчика, • требования к защищаемому файлу, варианты лицензирования.	6	Устный опрос № 2

№ раздела дисциплины	Перечень вопросов для самостоятельного изучения	Объем, акад. часы	Форма контроля
2	<p>Хранение конфиденциальных данных пользователей в аппаратных ключах серий eToken и ruToken.</p> <ul style="list-style-type: none"> • развертывание Центра сертификации; • использование ключей eToken; <p>использование ruToken.</p>	10	Устный опрос № 2
3	<p>Развертывания и администрирование виртуальной защищенной частной сети ПО VipNet CUSTOM</p> <ul style="list-style-type: none"> • назначение и настройка ЦУС; • назначение и настройка УКЦ; <p>файл дистрибутив DST.</p>	10	Устный опрос №3
3,4	<p>Аппаратные ключи защиты серии e-token. Получить практический навык работы с электронными цифровыми сертификатами. Сохранение электронных цифровых сертификатов в аппаратных токенах e-token. Стандартные операции работы с цифровыми сертификатами: выпуск сертификата, работа с цифровым сертификатом, продление срока действия электронного цифрового сертификата, отзыв электронного цифрового сертификата. Развертывание и администрирование защищенных виртуальных частных сетей (на примере ПО VipNet)</p>	20	Устный опрос №3
4	<p>Выбор начальных граничных условий, характера обратной связи в системе управления исследуемого объекта</p> <ul style="list-style-type: none"> • уровни деградации, парируемые неисправности и ошибки, • схема проектной оценки надежности программного комплекса, <p>расчет исходного числа дефектов.</p>	10	Устный опрос №3

№ раздела дисциплины	Перечень вопросов для самостоятельного изучения	Объем, акад. часы	Форма контроля
5	Изучение системы имитационного моделирования, CALS технологии. задачи имитационного моделирования, область применимости имитационного моделирования, описание физической и математической модели управляющей системы, основные направления обеспечения надежности программных комплексов. Стратегия CALS технологии, как: • применение современных информационных технологий; • реинжиниринг бизнес-процессов; • применение методов "параллельной" разработки; • стандартизацию в области совместного использования данных и электронного обмена данными.	10	Устный опрос №3
5,6	Аппаратные ключи защиты серии gu-token. Получить практический навык работы с электронными цифровыми сертификатами. Сохранение электронных цифровых сертификатов в аппаратных токенах gu-token. Стандартные операции работы с цифровыми сертификатами. Обработка данных эксперимента, визуализация данных, создание компьютерной презентации.	20	Контрольная работа №1
6	Моделирование работы объекта и системы управления <ul style="list-style-type: none"> • режимы функционирования объекта, • переходные режимы, особенности моделирования, • надежность и критерии надежности, виды резервирования, структурное, функциональное, временное, информационное и алгоритмическое резервирование.	4	Устный опрос № 4
6	Анализ экспериментальных данных. Визуализация полученных данных. <ul style="list-style-type: none"> • Особенности получения экспериментальных данных: • Современные подходы к технологии визуализации данных, 2D и 3D модели; Использование анимации.	6	Устный опрос № 4

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

Методические указания для обучающихся по организации самостоятельной работы по дисциплине, включая перечень тем самостоятельной работы, формы текущего контроля по дисциплине и требования к их выполнению размещены в электронной информационно-образовательной среде СПбГТИ(ТУ) на сайте: <https://media.technolog.edu.ru>.

6. Фонд оценочных средств для проведения промежуточной аттестации.

Промежуточная аттестация по дисциплине проводится в форме зачета и защиты курсовой работы.

Зачет предусматривает выборочную проверку освоения предусмотренных элементов компетенции и комплектуется теоретическими вопросами.

При сдаче зачета студент получает два вопроса из перечня вопросов, время подготовки студента к устному ответу – до 30 мин.

Пример варианта вопросов на зачете:

Вариант № 1

1. Общая концепция защиты сетевых ресурсов, файлов, баз данных, конфиденциальной информации пользователей. Необходимость комплексного подхода?
2. Использование программных и программно-аппаратных средств защиты – достоинства и недостатки каждого из решений?

Результаты освоения дисциплины считаются достигнутыми, если для всех элементов компетенции достигнут пороговый уровень освоения компетенции на данном этапе – «зачет».

7. Перечень учебных изданий, необходимых для освоения дисциплины

а) печатные издания:

1. Ананченко, И.В. Аппаратные ключи eToken. Средство защиты eToken Network Logon: Практикум / И. В. Ананченко ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный технологический институт (технический университет), Кафедра системного анализа. - Санкт-Петербург : СПбГТИ (ТУ), 2015. – 26 с.
2. Норенков, И. П. Автоматизированные информационные системы: учеб. пособие для студ. вузов, обуч. по направлению 230100«Информатика и вычислительная техника» (УМО) / И. П. Норенков. - Москва: МГТУ им. Н. Э. Баумана, 2011. - 343 с. – ISBN 978-5-7038-3446-6.

б) электронные учебные издания:

1. Лопатин, В. М. Информатика для инженеров : учебное пособие / В. М. Лопатин. — Санкт-Петербург : Лань, 2019. - 172 с. – ISBN 978-5-8114-3463-3. - Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/book/115517> (дата обращения: 30.04.2020). - Режим доступа: по подписке.
2. Орлова, И. В. Информатика. Практические задания : учебное пособие / И. В. Орлова. - Санкт-Петербург : Лань, 2019. - 140 с. - ISBN 978-5-8114-3608-8. - Текст :

электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/book/113400> (дата обращения: 30.04.2020). - Режим доступа: по подписке.

3. Ананченко, И.В. Использование ключей серии HASP HL для защиты информации. Защита программного обеспечения: Методические указания / И. В. Ананченко; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный технологический институт (технический университет), Кафедра системного анализа. - Санкт-Петербург: СПбГТИ(ТУ), 2012. – 69 с. // СПбГТИ. Электронная библиотека. – URL: <https://technolog.bibliotech.ru> (дата обращения : 25.03.2021). Режим доступа: для зарегистрированных пользователей.

8. Перечень электронных образовательных ресурсов, необходимых для освоения дисциплины.

Учебный план, РПД и учебно-методические материалы: <http://media.technolog.edu.ru>.

Электронно-библиотечные системы:

«Электронный читальный зал – БиблиоТех»: <https://technolog.bibliotech.ru/>;

«Лань»: <https://e.lanbook.com/books/>.

Для расширения знаний по дисциплине рекомендуется использовать Интернет-ресурсы: проводить поиск в системах, таких как www.rambler.ru; www.yandex.ru; www.yahoo.ru; www.google.ru и использовать материалы сайтов, рекомендованных преподавателем на лекционных занятиях.

9. Методические указания для обучающихся по освоению дисциплины.

Все виды занятий по дисциплине «Современные компьютерные технологии в науке и защита интеллектуальной собственности» проводятся в соответствии с требованиями следующих СТП (СТО):

СТП СПбГТИ 040-02 КС УКДВ. Виды учебных занятий. Лекция. Общие требования;

СТО СПбГТИ 018-2014 КС УКДВ. Виды учебных занятий. Семинары и практические занятия. Общие требования к организации и проведению;

СТО СПбГТИ 020-2011. КС УКДВ. Виды учебных занятий. Лабораторные занятия. Общие требования к организации и проведению.

СТП СПбГТИ 048-2009 КС УКДВ. Виды учебных занятий. Самостоятельная планируемая работа студентов. Общие требования к организации и проведению.

СТП СПбГТИ 044-2012. КС УКДВ. Виды учебных занятий. Курсовой проект. Курсовая работа. Общие требования.

Планирование времени, необходимого на изучение данной дисциплины, лучше всего осуществлять на весь семестр, предусматривая при этом регулярное повторение пройденного материала.

Основными условиями правильной организации учебного процесса для студентов является:

плановость в организации учебной работы;

серьезное отношение к изучению материала;

постоянный самоконтроль.

На занятиях студент должен приходиться, имея знания по уже изученному материалу.

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

10.1. Информационные технологии.

В учебном процессе по данной дисциплине предусмотрено использование информационных технологий:

чтение лекций с использованием слайд-презентаций;

взаимодействие с обучающимися посредством электронной информационно-образовательной среды.

10.2. Программное обеспечение.

Microsoft Office (Microsoft Excel); программно-аппаратные и программные средства для установки защиты (ПО для работы с HASP (HL, SL), eToken, ruToken, Guardant на сервере и рабочих станциях.

10.3. Базы данных и информационные справочные системы.

Справочно-поисковая система «Консультант-Плюс».

11. Материально-техническое обеспечение освоения дисциплины в ходе реализации образовательной программы.

Для ведения лекционных занятий используется аудитория, оборудованная проектором, экраном, ноутбуком, на 100 посадочных мест.

Для ведения практических занятий используется компьютерный класс, оборудованный персональными компьютерами, объединенными в сеть.

12. Особенности освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья.

Для инвалидов и лиц с ограниченными возможностями учебные процесс осуществляется в соответствии с Положением об организации учебного процесса для обучения инвалидов и лиц с ограниченными возможностями здоровья СПбГТИ(ТУ), утвержденным ректором 28.08.2014.

**Фонд оценочных средств
для проведения промежуточной аттестации по
дисциплине
«Современные компьютерные технологии в науке и защита интеллектуальной
собственности»**

1. Перечень компетенций и этапов их формирования.

Индекс компетенции	Содержание	Этап формирования
ОПК-3	Способен решать задачи системного анализа и управления в технических системах на базе последних достижений науки и техники	промежуточный
ОПК-5	Способен решать задачи в области развития науки, техники и технологии, применяя современные методы системного анализа и управления с учетом нормативно-правового регулирования в сфере интеллектуальной собственности	промежуточный

2. Показатели и критерии оценивания компетенций на различных этапах их формирования, шкала оценивания

Код и наименование индикатора достижения компетенции	Показатели сформированности (дескрипторы)	Критерий оценивания	Уровни сформированности (описание выраженности дескрипторов)		
			«удовлетворительно» (пороговый)	«хорошо» (средний)	«отлично» (высокий)
ОПК-3.1 Использование современных компьютерных технологий в задачах системного анализа	<p>Знает современные компьютерные средства для решения задач системного анализа (ЗН-1).</p> <p>Умеет применять современные компьютерные средства для решения задач системного анализа (У-1).</p> <p>Владеет методами использования компьютерных технологий для решения прикладных научно-технических задач, в том числе системного анализа. (Н-1).</p>	Ответы на вопросы №1 - 6 к зачету	Демонстрирует слабые навыки применения современных компьютерных средств, для решения задач системного анализа Затрудняется с решением задач системного анализа, связанных с методами применения современных компьютерных технологий.	Демонстрирует с ошибками навыки владения современными программными средствами Справляется с решением задач системного анализа, связанных с методами применения современных компьютерных технологий.	Демонстрирует глубокие знания о современных программных средствах Справляется с решением задач системного анализа, связанных с методами применения современных компьютерных технологий. Демонстрирует глубокие знания принципов и подходов к применению компьютерных технологий.

Код и наименование индикатора достижения компетенции	Показатели сформированности (дескрипторы)	Критерий оценивания	Уровни сформированности (описание выраженности дескрипторов)		
			«удовлетворительно» (пороговый)	«хорошо» (средний)	«отлично» (высокий)
<p>ОПК-3.2 Исследование современных систем управления в технических системах</p>	<p>Знает методы создания сложных комплексов с использованием CASE-средств; знать, как контролировать качество разрабатываемых систем управления (ЗН-2). Умеет составлять модель по словесному описанию, настраивать модель, представлять модель в алгоритмическом и математическом виде; творчески использовать инструменты подготовки и принятия решений для системного анализа объектов химической технологии на основе лицензионных программных комплексов (У-2). Владет навыками использования инструментов для подготовки и принятия решений для системного анализа объектов химической технологии на основе лицензионных программных комплексов (Н-2).</p>	<p>Ответы на вопросы №7 - 11 к зачету</p>	<p>Демонстрирует слабые навыки владения методами создания сложных комплексов с использованием CASE-средств; Затрудняется с методами контроля качества разрабатываемых систем управления</p>	<p>Демонстрирует с ошибками навыки владения методами создания сложных комплексов с использованием CASE-средств. Справляется с решением задач системного анализа, для подготовки и принятия решений на основе лицензионных программных комплексов</p>	<p>Демонстрирует глубокие знания, навыки владения методами создания сложных комплексов с использованием CASE-средств. Демонстрирует глубокие знания принципов решения задач системного анализа, для подготовки и принятия решений на основе лицензионных программных комплексов.</p>

Код и наименование индикатора достижения компетенции	Показатели сформированности (дескрипторы)	Критерий оценивания	Уровни сформированности (описание выраженности дескрипторов)		
			«удовлетворительно» (пороговый)	«хорошо» (средний)	«отлично» (высокий)
ОПК-5.1 Использование современных компьютерных технологий в задачах системного анализа	<p>Знает методы и способы формализации объектов, процессов, явлений и реализации их на компьютере и способами представления информации о моделируемых объектах и их свойств в компьютере (ЗН-3).</p> <p>Умеет использовать прикладные системы ограничения доступа к научно-технической информации; выполнять поиск научной и научно-технической информации в компьютерных сетях и специализированных базах данных (У-3).</p> <p>Владеет навыками обеспечения информационной безопасности и защиты компьютеров и компьютерных сетей (Н-3).</p>	<p>Ответы на вопросы №12 - 26 к зачету</p>	<p>Демонстрирует слабые навыки владения современными программными средствами. Затрудняется с решением задач системного анализа, связанных с методами применения современных компьютерных технологий.</p>	<p>Демонстрирует с ошибками навыки владения современными программными средствами</p> <p>Справляется с решением задач системного анализа, связанных с методами применения современных компьютерных технологий.</p>	<p>Демонстрирует глубокие знания о современных программных средствах</p> <p>Справляется с решением задач системного анализа, связанных с методами применения современных компьютерных технологий.</p> <p>Демонстрирует глубокие знания принципов и подходов к применению компьютерных технологий с учетом норм регулирования интеллектуальной собственности.</p>

Код и наименование индикатора достижения компетенции	Показатели сформированности (дескрипторы)	Критерий оценивания	Уровни сформированности (описание выраженности дескрипторов)		
			«удовлетворительно» (пороговый)	«хорошо» (средний)	«отлично» (высокий)
ОПК-5.2 Применение современных программных средств с учетом норм регулирования интеллектуальной собственности	Знает принципы применения современных программных средств с учетом норм регулирования интеллектуальной собственности (ЗН-4). Умеет внедрять методы применения современных программных средств с учетом норм регулирования интеллектуальной собственности (У-4). Владеет методами анализа применения современных программных средств с учетом норм регулирования интеллектуальной собственности (Н-4).	Ответы на вопросы №27 - 34 к зачету; защита курсовой работы	Затрудняется в четком определении принципов и подходов применения современных программных средств с учетом норм регулирования интеллектуальной собственности. Демонстрирует слабые навыки внедрения современных программных средств с учетом норм регулирования интеллектуальной собственности. Затрудняется с решением задач, связанных с методами применения современных программных средств с учетом норм регулирования интеллектуальной собственности.	Определяет основные принципы и подходы к применению современных программных средств с учетом норм регулирования интеллектуальной собственности. Демонстрирует с ошибками навыки внедрения современных программных средств с учетом норм регулирования интеллектуальной собственности. Справляется с решением типовых задач, связанных с методами применения современных программных средств с учетом норм регулирования интеллектуальной собственности.	Демонстрирует глубокие знания принципов и подходов к применению современных программных средств с учетом норм регулирования интеллектуальной собственности. Демонстрирует хорошие навыки внедрения современных программных средств. Демонстрирует хорошие навыки и умения решения задач, связанных с методами применения современных программных средств с учетом норм регулирования интеллектуальной собственности.

Шкала оценивания соответствует СТО СПбГТИ (ТУ).

Шкала оценивания курсовой работы – балльная («отлично», «хорошо», «удовлетворительно», «неудовлетворительно»).

Шкала оценивания на зачете – «зачет», «незачет». При этом «зачет» соотносится с пороговым уровнем сформированности компетенций.

3. Типовые контрольные задания для проведения промежуточной аттестации

а) Вопросы для оценки сформированности элементов компетенции ОПК-3:

1. Общая концепция защиты сетевых ресурсов, файлов, баз данных, конфиденциальной информации пользователей. Необходимость комплексного подхода?
2. Использование электронных цифровых сертификатов, шифрование?
3. Использование программных и программно-аппаратных средств защиты – достоинства и недостатки каждого из решений?
4. Современные компьютерные технологии в науке, направленные на защиту информации, представляющей научную и коммерческую ценность.
5. Обработка данных эксперимента, визуализация данных, создание компьютерной презентации.
6. Защита информации от случайного или преднамеренного уничтожения, создание резервных копий?
7. VPN – технологии, защита компьютерных сетей?
8. Роль эксперимента в оценке надежности. Классификация методов статистических испытаний надежности.
9. Сохраняемость. Долговечность. Система и элемент. Структурное, функциональное, временное, информационное и алгоритмическое резервирование.
10. Анализ устойчивости моделируемой системы управления.
11. Современные технологии визуализации процессов моделирования, представление исходных данных и полученных результатов в форматах, облегчающих восприятие информации.

б) Вопросы для оценки сформированности элементов компетенции ОПК-5:

12. Назначение комплекса eToken Network Logon, основные характеристики?
13. Решение проблемы "слабых" паролей с помощью eToken Network Logon?
14. USB-ключи серии eToken - eToken ГОСТ, eToken PRO (Java), КриптоПро eToken CSP - основные характеристики, возможность использования с eToken Network Logon?
15. USB-ключи серии eToken - eToken NG-FLASH (Java), eToken NG-OTP (Java) – основные характеристики, возможность использования с eToken Network Logon?
16. Специализированный USB-ключ – eToken PRO Anywhere. Основные характеристики, назначение, возможность использования с eToken Network Logon?
17. Порядок установки и администрирования eToken Network Logon?
18. Модели эффективности отладки.
19. Модели потоков инициирующих событий.
20. Вероятность проявления дефекта при однократном выполнении ФСО.
21. Вероятность проявления дефекта при многократном выполнении ФСО.
22. Вероятность безотказной работы ПК в режиме МКЦП при случайном потоке инициирующих событий. Учет процедур парирования ошибок.
23. Оценка надежности программного комплекса по результатам отладки и нормальной эксплуатации.
24. Основные направления обеспечения надежности программных комплексов.
25. Уровни деградации, парируемые неисправности и ошибки. Общая схема проектной оценки надежности программного комплекса. Расчет исходного числа дефектов.
26. Расчет остаточного числа дефектов после автономной и комплексной отладки. Оценка вероятности проявления дефекта при однократном выполнении ФСО.
27. Оценка вероятности проявления дефекта при многократном выполнении ФСО. Оценка характеристик потоков инициирующих событий.
28. Модели распределения числа дефектов в алгоритмах и базах данных.
29. CASE-технологии. Стандарты ISO, SW-CMM. CASE-технологии. Развитие методологии проектирования.

30. Моделирование работы объекта и системы управления. Надежность. Критерии и показатели надежности.
31. Работоспособность. Отказ. Неисправность. Восстановление. Безотказность. Ремонтопригодность. Сохраняемость. Долговечность. Система и элемент.
32. Факторы, влияющие на надежность аппаратно-программного комплекса.
33. Факторы, влияющие на надежность программного обеспечения.
34. Виды резервирования. Структурное, функциональное, временное, информационное и алгоритмическое резервирование.

При сдаче зачета студент получает два вопроса из перечня, приведенного выше.

Время подготовки студента к устному ответу на вопросы – до 30 мин.

Темы и содержание контрольных работ

Контрольная работа № 1 «Аппаратные ключи eToken. Средство защиты EToken Network Logon»

Привести общую характеристику ключей eToken. Элементы стартового окна входа после установки дистрибутива eToken Network Logon. Ввод пароля от существующей учётной записи или выбор варианта входа с использованием eToken? Создание нового профиля. Назначение комплекса eToken Network Logon, основные характеристики? Решение проблемы "слабых" паролей с помощью eToken Network Logon? USB-ключи серии eToken - eToken ГОСТ, eToken PRO (Java), КриптоПро eToken CSP - основные характеристики, возможность использования с eToken Network Logon? USB-ключи серии eToken - eToken NG-FLASH (Java), eToken NG-OTP (Java) – основные характеристики, возможность использования с eToken Network Logon? Специализированный USB-ключ – eToken PRO Anywhere. Основные характеристики, назначение, возможность использования с eToken Network Logon? Порядок установки и администрирования eToken Network Logon?

Контрольная работа № 2 «Использование ключей серии HASP HL для защиты информации. Защита программного обеспечения».

Изучение использования ключей серии HASP HL для защиты информации. Защита программного обеспечения. Установить на компьютере программный комплекс HASP Studio для защиты информации. Используя методические указания к установленному комплексу научиться защищать исполняемые программные файлы exe типа. Ознакомиться с возможностями программного комплекса «HASP Studio». Выполнение работы. Используя установленный программный комплекс и методические указания выполнить следующие этапы работы - последовательность типовых действий установки и менеджмента защищаемого программного обеспечения с использованием технологии HASP SPM:

Этап 1 – Подготовительный этап. Содержит инструкции по установке системы HASP SRM и запуску HASP SRM Vendor Suite.

Этап 2 – Определение компонентов ПО. Перед установкой защиты определяем приложения, как отдельные компоненты.

Этап 3 – Установка защиты. Выполняем установку защиты на приложения и компоненты, определенные на предыдущем этапе.

Этап 4 – Формирование программного пакета. Создание готового программного пакета на базе имеющихся компонентов и приложений.

Этап 5 – Создание условно-бесплатной версии. Создание в HASP SRM Business Studio условно-бесплатной версии для одного из компонентов программного продукта.

Этап 6 – Оформление и обработка заказов. Оформление заказов на созданные продукты и внесение данных о поставщиках. Создаем обновления лицензий для установленных продуктов.

Этап 7 – Работа с защищенным приложением на стороне пользователя. Изучение работы с приложениями, защищенными с помощью HASP SRM, на стороне пользователя.

Подготовить отчет по выполненной работе. Объяснить механизм работы защиты, схемы лицензирования защищенного ПО.

Ответить на контрольные вопросы

1. Построение защиты на основе использования Hasp Envelope. Достоинства и недостатки?
2. Как действия выполняются на подготовительном этапе и этапе создания компонентов?
3. Какие действия выполняются на этапе формирования программного пакета и этапе создания условно-бесплатной версии?
4. Какие действия необходимо выполнить на этапе оформления и обработки заказов?
5. Типовые действия по работе с защищенным приложением, выполняемые на стороне пользователя после получения им защищенной программы?

Темы курсовых работ

Тематика курсовых работ связана с использованием современных программно-аппаратных средств обеспечения информационной безопасности.

Примерные темы работ:

1. Установка и администрирование навесной защиты исполняемых приложений (com, exe, dll) с помощью комплекта разработчика Sentinel LDK 7.6
2. Установка и администрирование встраиваемой защиты приложений с помощью комплекта разработчика Sentinel LDK 7.6
3. Защита доступа к сайту в сети Интернет с помощью ключа РутOKEN Web.
4. Использование аппаратных токенов (eToken, ruToken) для работы с электронной цифровой подписью (ЭЦП).
5. Развертывание VPN сетей, использование ключей серий eToken и ruToken для усиления защищённости VPN сети.
6. Использование аппаратных токенов (eToken, ruToken) для защиты контента веб серверов.
7. Лизинг программного обеспечения с использованием технологии защита программного обеспечения программно-аппаратными ключами марки HASP HL TimeNet (комплект разработчика Sentinel LDK 7.6).
8. Использование аппаратных ключей для защиты СУБД и информационного контента БД.
9. Установка и настройка Центра сертификации, использование ключей eToken в домене Windows 2016
10. Сопровождение функционирования Центра сертификации, повышение защищенности систем на основе Windows 2016 с использованием аппаратных ключей защиты.

4. Методические материалы для определения процедур оценивания знаний, умений и навыков, характеризующих этапы формирования компетенций.

Промежуточная аттестация по дисциплине проводится в соответствии с требованиями СТП:

СТО СПбГТИ(ТУ) 016-2015 КС УКДВ. Порядок организации и проведения зачетов и экзаменов.

СТП СПбГТИ 044-2012. КС УКВД. Виды учебных занятий. Курсовой проект. Курсовая работа. Общие требования.