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
«_____» _____ 2019 г.

Рабочая программа дисциплины

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Направление подготовки

09.03.02Информационные системы и технологии

Направленность программы бакалавриата

Информационные системы и технологии

Квалификация

Бакалавр

Форма обучения

Очная

Факультет **информационных технологий и управления**

Кафедра**системного анализа и информационных технологий**

Санкт-Петербург

2019

ЛИСТ СОГЛАСОВАНИЯ

Должность разработчика	Подпись	Ученое звание, фамилия, инициалы
доцент		доцент,АнанченкоИ.В.

Рабочая программа дисциплины «Программно-аппаратные средства обеспечения безопасности информационных систем» обсуждена на заседании кафедры системного анализа и информационных технологий
протокол от «___» _____2019 № __
Заведующий кафедрой А.А. Мусаев

Одобрено учебно-методической комиссией факультета информационных технологий и управления
протокол от «___» _____2019 № __

Председатель В.В. Куркина

СОГЛАСОВАНО

Руководитель направления подготовки «Информационные системы и технологии»		Г.А. Мамаева
Директор библиотеки		Т.Н.Старостенко
Начальник методического отдела учебно-методического управления		Т.И.Богданова
Начальник учебно-методического управления		С.Н.Денисенко

СОДЕРЖАНИЕ

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 обучающийся должен овладеть следующими результатами обучения по дисциплине:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения (дескрипторы)
• **ПК-7** Способен управлять безопасностью сетевых устройств и ПО	**ПК-7.1** Управление безопасностью сетевых устройств	**Знать:** - принципы и подходы к управлению безопасностью сетевых устройств(ЗН-1). **Уметь:** - внедрятьметодыуправления безопасностью сетевых устройств(У-1). **Владеть:** - методами анализа для решения задач, связанных с управлением безопасностью сетевых устройств.(Н-1).

2. Место дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам базовой части,формируемой участниками образовательных отношений (Б1.В.16) и изучается на 4 курсе в 7 семестре.

Изучение данной дисциплины базируется на знании студентами основ математики, информатики и основ алгоритмизации, на знаниях, полученных в процессе изучения дисциплин «Операционные системы», «Информатика», «Алгоритмы и структуры данных», «Программирование на языке С++», «Программирование на языках низкого уровня», «Программирование на языке Python», «Архитектура информационных систем»,«Мультимедиа технологии», «Облачные технологии»,«Корпоративные информационные системы».

Полученные в процессе изучения дисциплины«Программно-аппаратные средства обеспечения безопасности информационных систем» знания, умения и навыки могут быть использованы при изучении дисциплин «Методы и средства проектирования информационных систем и технологий», «Информационная безопасность», а также в научно-исследовательской работе бакалавра и при выполнении выпускной квалификационной работы.

3. Объем дисциплины

Вид учебной работы	Всего, академических часов
	Очная форма обучения
Общая трудоемкость дисциплины (зачетных единиц/ академических часов)	3/ 108
Контактная работа с преподавателем:	**58**
занятия лекционного типа	**18**
занятия семинарского типа, в т.ч.	36
семинары, практические занятия	**36**
лабораторные работы	**-**
курсовое проектирование (КР или КП)	
КСР	**4**
другие виды контактной работы	
Самостоятельная работа	50
Форма текущего контроля (Кр, реферат, РГР, эссе)	-
Форма промежуточной аттестации (КР, КП, зачет, экзамен)	**зачет**

4. Содержание дисциплины

4.1. Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Занятия лекционного типа, акад. часы	Занятия семинарского типа, академ. часы		Самостоятельная работа, акад. часы	Формируемые компетенции	Формируемые индикаторы
			Семинары и/или практические занятия	Лабораторные работы			
1.	Развертывание и администрирование защищенных виртуальных частных сетей. Защита рабочего места оператора информационной системы с использованием программно-аппаратного решения JaCartaSecurLogon	6	9		14	ПК-7	ПК-7.1
2	Использование программных и аппаратных ключей серии HASPHLиHASPSL для защиты программного обеспечения	4	9		12	ПК-7	ПК-7.1
3.	Использование программных и аппаратных ключей сери GUARDANTдля защиты программного обеспечения	4	9		12	ПК-7	ПК-7.1
4.	Использование ключей серий eTokenиruTokenдля шифрования информации и ЭЦП	4	9		12	ПК-7	ПК-7.1

4.2. Занятия лекционного типа

№ раздела дисци-	Наименование темы и краткое содержание занятия	Объем, акад. часы	Инновационная форма
1.	Развертывание виртуальной частной сети. Развертывание виртуальной защищенной частной сети.На примере ПО VipNet CUSTOM развертывание и администрирование виртуальной защищенной частной сети. JaCarta SecurLogon — сертифицированное программно-аппаратное решение, позволяющее осуществить простой и быстрый переход от однофакторной аутентификации на основе пары логин-пароль к двухфакторной аутентификации при входе в операционную систему и доступе к сетевым ресурсам за счёт использования USB-токенов и смарт-карт.JaCarta SecurLogon —установка, послеустановочная настройка, администрирование.Комплект разработчика Rutoken. Электронные идентификаторы Рутокен Web.	6	ЛВ
2.	Использование программных и аппаратных ключей серии Sentinel HL и Sentinel SL (HASPHL, HASPSL) для защиты программного обеспечения.Защита программного обеспечения программно-аппаратными ключами марки Sentinel HL. Защита сетевого программного обеспечения информационных систем программно-аппаратными ключами марки Sentinel HL Net. Лизинг программного обеспечения информационных систем с использованием технологии защита программного обеспечения программно-аппаратными ключами марки Sentinel HL Time. Защита программного обеспечения с помощью защиты навесного типа с использованием аппаратного ключа защиты серии Sentinel.	4	ЛВ
3.	Использование программных и аппаратных ключей серии GUARDANT для защиты программного обеспечения информационных систем.Защита программного обеспечения с помощью защиты навесного типа с использованием аппаратного ключа защиты серии CUARDANT: установка инструментария разработчика,требования к защищаемому файлу,варианты лицензирования.	4	ЛВ
4.	Использование ключей серий eToken и ruToken для шифрования информации и ЭЦП.Хранение и использование 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.	4	ЛВ

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	JaCarta SecurLogon — установка, послеустановочная настройка, администрирование. Развертывание виртуальной защищенной частной сети. На примере ПО VipNet CUSTOM формируется практические навыки развертывания и администрирования виртуальной защищенной частной сети. Развертывание виртуальной защищенной частной сети VPN. ViPNet Client – установка, конфигурирование, защита, ключевая “дискета”, ключевой набор. Администрирование виртуальной защищенной частной сети VPN – «Деловая почта». Получение практического навыка работы с приложением «Деловая почта», автопроцессинг, ЭЦП; типовые схемы применения ПО ViPNet.	9	Слайд-презентация, групповая дискуссия
2	Защита исполняемых exe файлов с помощью навесной защиты Sentinel. Получение практических навыков работы с Sentinel ключами и программным обеспечением SentinelSDKVendor Suite. Защита исполняемых exe файлов. Организация встроенной защиты программы, написанной на Visual Studio с помощью SENTINEL, практические навыки работы с Sentinel HASP API, установить встроенную защиту в программу, созданную средствами языка Visual Studio и/или Delphi. Выполнить чтение и запись данных на аппаратный ключ. Защита DLL библиотек с помощью Sentinel. Разработать программу средствами Visual Studio, использующую динамически подключаемую библиотеку DLL, защищенную с помощью Sentinel.	9	Слайд-презентация, групповая дискуссия
3	Защита исполняемых exe файлов с помощью навесной защиты Guardant, получение практических навыков работы с Guardant ключами и программным обеспечением Guardant. Защита исполняемых exe файлов. Защита DLL библиотек с помощью Guardant. Разработать программу средствами Visual Studio, использующую динамически подключаемую библио-	9	Слайд-презентация, групповая дискуссия

№ раздела дисциплины	Наименование темы и краткое содержание занятия	Объем, акад. часы	Инновационная форма
4	Аппаратные ключи защиты серии e-token. 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. Аппаратные ключи защиты серии ru-token, навык работы с электронными цифровыми сертификатами. Сохранение электронных цифровых сертификатов в аппаратных токенах ru-token. Стандартные операции работы с цифровыми сертификатами: выпуск сертификата, работа с цифровым сертификатом, продление срока действия электронного цифрового сертификата, отзыв электронного цифрового сертификата.	9	Слайд-презентация, групповая дискуссия

4.4. Самостоятельная работа обучающихся

№ раздела дисциплины	Перечень вопросов для самостоятельного изучения	Объем, акад. часы	Форма контроля
1	JaCarta SecurLogon — сертифицированное программно-аппаратное решение, позволяющее осуществить простой и быстрый переход от однофакторной аутентификации на основе пары логин-пароль к двухфакторной аутентификации при входе в операционную систему и доступе к сетевым ресурсам за счёт использования USB-токенов и смарт-карт.JaCarta SecurLogon —установка, послеустановочная настройка, администрирование. Развертывания и администрирование виртуальной защищенной частной сети.	9	Устный опрос №1
2	Защита программного обеспечения с помощью защиты навесного типа с использованием аппаратного ключа защиты серии HASP: представители ключей серии HASP HL, использование HASP Envelope, модели лицензирования ПО. Защита программного обеспечения с помощью защиты встраиваемого типа с использованием аппаратного ключа защиты серии SENTINEL. Подключение библиотек защиты SENTINEL на уровне исходного кода, особенности встраиваемой защиты для выбранного языка программирования.	9	Устный опрос №2

№ раздела дисциплины	Перечень вопросов для самостоятельного изучения	Объем, акад. часы	Форма контроля
3	Защита программного обеспечения (библиотечных dll модулей) с помощью защиты встраиваемого типа с использованием аппаратного ключа защиты серии SENTINEL,Guardant, HASP: структура защищаемых dll библиотек, анализ схемы защиты dll, особенности модели лицензирования. Защита программного обеспечения с помощью защиты навесного типа с использованием аппаратного ключа защиты серии Guardant: установка инструментария разработчика, требования к защищаемому файлу,варианты лицензирования.	9	Устный опрос №3
4	Хранение конфиденциальных данных пользователей в аппаратных ключах серий eToken и ruToken. Развертывание Центра сертификации: использование ключей eToken; использование ruToken.Развертывания и администрирование виртуальной защищенной частной сети ПО.	9	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: http://media.technolog.edu.ru

6. Фонд оценочных средств для проведения промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в виде зачета.

Зачет предусматривает выборочную проверку освоения предусмотренных элементов компетенций и комплектуется теоретическими вопросами (для проверки знаний, умений и навыков).

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

Пример варианта вопросов на зачете:

Вариант № 1

1. Основные компоненты системы защиты информации с использованием VPN: определение, состав, характеристики, требования?
2. Как защитить исполняемый файл exe структуры информационной системы, используя навесную защиту, базирующуюся на применении ключа Sentinel?

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

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 ; СПбГТИ(ТУ). Каф. систем. анализа. – СПб. : [б. и.], 2015. – 26 с. : ил. – Библиогр.: с. 26.
2. Норенков, И. П. Автоматизированные информационные системы: Учебное пособие для вузов по направлению 230100 "Информатикаи вычислительная техника" / И. П. Норенков. – М. : Изд-во МГТУ им. Н.Э.Баумана, 2011. – 342 с.

б) электронные учебные издания:

1. Набиуллина, С. Н. Информатика и ИКТ. Курс лекций: учебное пособие / С. Н. Набиуллина. – СПб; М.; Краснодар: Лань, 2019. – 72 с. (ЭБС Лань)
2. Лопатин, В.М. Информатика для инженеров: Учебное пособие / В. М. Лопатин. – СПб; М.; Краснодар: Лань, 2019. – 172 с. (ЭБС Лань)
3. Орлова, И.В. Информатика. Практические задания: Учебное пособие / И. В. Орлова. – СПб; М.; Краснодар: Лань, 2019. – 140 с. (ЭБС Лань)
4. Ананченко, И.В. Использование ключей серии HASP HL для защиты информации. Защита программного обеспечения: Методические указания / И. В. Ананченко; СПбГТИ(ТУ). Каф. систем. анализа. – Электрон. текстовые дан. – СПб. : [б. и.], 2012. – 69 с.: ил. – Библиогр.: с. 68 (ЭБ).

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/

9. Методические указания для обучающихся по освоению дисциплины

Все виды занятий по дисциплине «Корпоративные информационные системы» проводятся в соответствии с требованиями следующих СТП:

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.

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

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 занятия студент должен приходить, 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 ЭИОС.

10.2. Программное обеспечение

Программы: ОСMicrosoftWindows, ОСKaliLinux, ОСAstraLinux, ОСUbuntu, MathCAD, MicrosoftOffice (MicrosoftWord, MicrosoftExcel, MicrosoftAccess, MicrosoftPowerPoint), интегрированнаясредаMicrosoftVisualStudioCommunity.VMware Workstation Player. Hyper-V. MSVirtualPC.Комплект разработчика Sentinel LDK 7.10, Sentinel HASP 5.12.

10.3. Базы данных и информационно справочные системы

Справочно-поисковая система «Консультант-Плюс»

11. Материально-техническая база, необходимая для осуществления образовательногопроцесса по дисциплине.

Для ведения лекционных и практических занятий используетсякомпьютерный класс, оснащенный объединенными в сеть персональными компьютерами, оборудованием и техническими средствами обучения на необходимое количество посадочных мест. При проведении занятий используется аудитория, оборудованная при необходимости проектором для отображения презентаций. Кроме того, при проведении лекций и практических занятий необходим компьютер с установленным на нем браузером и программным обеспечением для демонстрации презентаций (Power Point и др.). Для самостоятельной работы с медиаматериалами каждому студенту требуется персональный компьютер или планшет, широкополосный доступ в сеть Интернет, браузер последней версии, устройство для воспроизведения звука (динамики, колонки, наушники и др.)

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 28.08.2014г.

Приложение № 1
к рабочей программе дисциплины

Фонд оценочных средств
для проведения промежуточной аттестации по
дисциплине «Программно-аппаратные средства обеспечения безопасности информационных систем»

1. Перечень компетенций и этапов их формирования.

Индекс компетенции	Содержание	Этап формирования
ПК-7	**Способен управлять безопасностью** сетевых устройств и **ПО**	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)
ПК-7.1 Управление безопасностью сетевых устройств	**Правильно определяет** принципы и подходы к управлению безопасностью сетевых устройств (ЗН-1).	Ответы на вопросы №1 - 23к зачету	Затрудняется в четком определениипринципов и подходов к управлению безопасностью сетевых устройств.	Определяетосновные-принципы и подходы к управлению безопасностью сетевых устройств.	Демонстрирует глубокие знания принципов и подходов к управлению безопасностью сетевых устройств.
	Демонстрирует навыкивнедрения методов управления безопасностью сетевых устройств (У-1).	Ответы на вопросы №1 - 23к зачету	Демонстрирует слабые навыки внедрения методов управления безопасностью сетевых устройств.	Демонстрирует с ошибками навыки внедрения методов управления безопасностью сетевых устройств.	Демонстрирует хорошие навыки применениянаметодов управления безопасностью сетевых устройств.
	Перечисляет и приводит примерырешения задач, связанных с управлением безопасностью сетевых устройств и программного обеспечения(Н-1).	Ответы на вопросы №1 - 23к зачету	Затрудняется с решением задач,связанных с управлением безопасностью сетевых устройств и программного обеспечения.	Справляется с решениемтиповых задач,связанных с управлением безопасностью сетевых устройств и программного обеспечения.	Демонстрирует хорошие навыки и умения решения задач,связанных с управлением безопасностью сетевых устройств и программного обеспечения.

Шкала оценивания соответствует СТО СПбГТИ(ТУ):

По дисциплине промежуточная аттестация проводится в форме зачета, шкала оценивания – балльная («отлично», «хорошо», «удовлетворительно», «неудовлетворительно»).

3. Типовые контрольные задания для проведения промежуточной аттестации

а) Вопросы для оценки знаний, умений и навыков, сформированных у студента по компетенции ПК-7:

1. Защита программного обеспечения с помощью ключа Sentinel HL?
2. Защита программного обеспечения с помощью ключа Guardant?
3. Защита программного обеспечения с помощью программного ключа Sentinel SL?
4. Защита программного обеспечения с помощью программного ключа Guardant SP?
5. Методы защиты информации в компьютерных сетях?
6. Администрирование защищенных VPN-сетей?
7. Администрирование защищенных виртуальных частных сетей (на примере ПО VipNet)?
8. Развертывание и администрирование защищенных VPN-сетей?
9. Электронные ключи Guardant. Электронный ключ Guardant Sign?
10. Электронный ключ Guardant Code. Лицензирование сетевых приложений. Защищенные схемы продаж?
11. Комплекты разработчика Guardant. Выбор модели ключа?
12. Шифрования данных и ЭЦП с помощью аппаратных ключей eToken?
13. Шифрования данных и ЭЦП с помощью аппаратных ключей ruToken?
14. ViPNet Administrator (Администратор). Особенности ключевой структуры VipNet.
15. Использование аппаратных ключей защиты eToken и HASP для защиты ПО и информации пользователей.
16. Ключевой и удостоверяющий центр VipNet Custom. Технология разграничения доступа к информации на примере ViPNet.
17. Частные сети (VPN): принципы построения, конфигурирование, варианты реализации.
18. Электронные ключи Guardant. Выбор модели ключа. Удаленное обновление памяти ключа.
19. ViPNet – сервер открытого Интернета. Транспортный модуль MFTP. Деловая почта. VPN как средство информационной защиты.
20. Центры сертификации – назначение, техническая реализация.
21. Виды угроз безопасности в ТКС. Криптографические системы и их использование в VipNet.
22. Комплект разработчика RuToken. Электронные идентификаторы Рутокен Web.
23. Защита рабочего места оператора информационной системы с использованием программно-аппаратного решения JaCartaSecurLogon.

При сдаче зачета, студент получает два вопроса сформированных на основе перечня, приведенного выше.Время подготовки студента к устному ответу на вопросы – до 30 мин.

5. 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 проведения зачетов и экзаменов.