

МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«Санкт-Петербургский государственный экономический университет»



Защита в операционных системах

Рабочая программа дисциплины

Направление подготовки/ Специальность	10.03.01 Информационная безопасность
Направленность (профиль) программы/ Специализация	Безопасность компьютерных систем (в экономике и управлении)
Уровень высшего образования	Бакалавриат
Форма обучения	очная
Год набора	2023

Составитель(и):

к.т.н, Чернокнижный Геннадий Михайлович

Часов по учебному плану	144	Виды контроля в семестрах: Экзамен: семестр 7
в том числе:		
контактная работа	64	
самостоятельная работа	44	
практическая подготовка	0	
часов на контроль	36	

Распределение часов дисциплины:

Семестр:	7
Вид занятий	Часы
Лекционные занятия	22
Практические занятия	
Лабораторные работы	42
Итого аудиторных часов	64
Самостоятельная работа	44
Часы на контроль	36
Итого академических часов	144
Общая трудоемкость в зачетных единицах	4

Санкт-Петербург
2023

СОДЕРЖАНИЕ

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	3
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	3
3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ	3
4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ*	3
5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ.....	4
5.1 Рекомендуемая литература	4
5.2 Перечень лицензионного и свободно распространяемого программного обеспечения, в т.ч. отечественного производства	5
5.3 Перечень информационных справочных систем (ИСС) и современных профессиональных баз данных (СПБД).....	5
6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ	5
7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩЕГОСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ.....	7
8. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ	8
ФОНД ОЦЕНОЧНЫХ СРЕДСТВ.....	10
1.1 Контрольные вопросы и задания к промежуточной аттестации	10
1.2 Темы письменных работ.....	10
1.3 Контрольные точки	10
1.4 Другие объекты оценивания	11
1.5 Самостоятельная работа обучающегося	11
1.6 Шкала оценивания результата	11

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель:	Дать студентам необходимые знания, умения и навыки защиты сетевых операционных систем с применением современных программно-аппаратных средств, необходимые для использования их в работе в компаниях, нуждающихся в защите конфиденциальной информации.
--------------	---

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.О Защита в операционных системах относится к обязательной части Блока 1.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Код и наименование компетенции выпускника	Код и наименование индикатора достижения компетенций	Планируемые результаты обучения по дисциплине
ОПК-1 - Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;	ОПК-1.1.02 - Способен применять методы гибкой настройки политик безопасности различных семейств операционных систем	<p>Знать: роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства.</p> <p>Уметь: применять методы гибкой настройки политик безопасности различных семейств операционных систем.</p> <p>Владеть: методиками настройки наложенных средств защиты информации в операционных системах.</p>

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ*

Номер и наименование тем и/или разделов/тем	Содержание дисциплины	Объем дисциплины (академические часы)			
		Контактная работа			СРО
		ЗЛТ	ПЗ	ЛР	
Тема 1. Модели безопасности сетевых операционных систем.	Анализ выполнения современными ОС формализованных требований к защите информации от НСД. Основные встроенные механизмы защиты ОС и их недостатки Анализ существующей статистики угроз для современных универсальных ОС. Семейства ОС и общая статистика угроз.	2			2

Тема 2. Система безопасности операционной системы Windows.	Способы защиты в файловых системах. Сервер аутентификации Kerberos. Протокол NTLM. Аутентификация в Windows.	2		10	6
Тема 3. Защита в операционной системе Linux.	Управление доступом к системе. Управление доступом к данным. Защита хранимых данных. Восстановление файловой системы.	6		16	14
Тема 4. Системы защиты программного обеспечения.	Классификация систем защиты ПО. Упаковщики/шифраторы. Системы защиты от несанкционированного копирования. Системы защиты от НСД. Обфускация и защита программных продуктов. Безопасность программного обеспечения и человеческий фактор.	6		8	8
Тема 5. Протоколирование и аудит.	Основные понятия. Аудит в Windows. Аудит в Linux. Системы бэкапа. Показатели эффективности систем защиты.	4		4	8
Тема 6. Безопасность операционных систем мобильных устройств.	Угрозы безопасности операционным системам мобильных устройств. Типичные вредоносные действия. Некорректно работающие приложения. Использование цифровых подписей.	2		4	6
Контроль:					36
Всего по дисциплине:		22	0	42	44

*ЗЛТ – занятия лекционного типа, ПЗ – все виды занятий семинарского типа, кроме лабораторных работ, ЛР – лабораторные работы, СРО – самостоятельная работа обучающегося

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Рекомендуемая литература

Библиографическое описание издания (автор, заглавие, вид, место и год издания, кол. стр.)	Электронные ресурсы
Чернокнижный Г.М., Васильева И.Н. Операционные системы. СПбГЭУ, 2018, 220с.	http://opac.unecon.ru/elibrary ... 81%D1%82%D0%B5%D0%BC%D1%8B.pdf
Чернокнижный Г.М. Вычислительные сети. Контроль безопасности в компьютерных сетях. СПбГЭУ, 2016, 98с.	http://opac.unecon.ru/elibrary ... 20%D1%81%D0%B5%D1%82%D0%B8.pdf
Таненбаум Э., Бос. Х. Современные операционные системы. 4-е изд. ? СПб.: Питер, 2015. ? 1120 с.	https://ibooks.ru/bookshelf/377414/reading
Чернокнижный Г.М. Безопасность операционных систем : учебное пособие / Г.М.Чернокнижный, И.Н.Васильева : СПбГЭУ, 2019	https://opac.unecon.ru/elibrar ... B8%D1%81%D1%82%D0%B5%D0%BC.pdf

5.2 Перечень лицензионного и свободно распространяемого программного обеспечения, в т.ч. отечественного производства

- 7-Zip
- Dallas Lock Linux (СЗИ НСД)
- Debian
- Git
- Oracle VM VirtualBox
- ОС Альт образование 10
- LibreOffice

5.3 Перечень информационных справочных систем (ИСС) и современных профессиональных баз данных (СПБД)

№	Наименование СПБД/ ИСС
1.	Электронная библиотека Grebennikon.ru – www.grebennikon.ru
2.	Научная электронная библиотека eLIBRARY – www.elibrary.ru
3.	Научная электронная библиотека КиберЛеника – www.cyberleninka.ru
4.	База данных ПОЛПРЕД Справочники – www.polpred.com
5.	База данных OECD Books, Papers & Statistics на платформе OECD iLibrary www.oecd-ilibrary.org
6.	Справочная правовая система КонсультантПлюс (инсталлированный ресурс СПбГЭУ или www.consultant.ru)
7.	Справочная правовая система «ГАРАНТ» (инсталлированный ресурс СПбГЭУ или www.garant.ru)
8.	Информационно-справочная система «Кодекс» (инсталлированный ресурс СПбГЭУ или www.kodeks.ru)
9.	Электронная библиотечная система BOOK.ru - www.book.ru
10.	Электронная библиотечная система ЭБС ЮРАЙТ – www.urait.ru
11.	Электронно-библиотечная система ЗНАНИУМ (ZNANIUM) – www.znanium.com
12.	Электронная библиотека СПбГЭУ – opac.unecon.ru

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации данной дисциплины имеются специальные помещения для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ) групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.

Помещения оснащены оборудованием и техническими средствами обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду университета.

Наименование учебных аудиторий, перечень	Адрес (местоположение) учебных аудиторий
<p>Ауд. 2062 Учебная аудитория (для проведения занятий лекционного типа и занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации), оборудована мультимедийным комплексом. Специализированная мебель и оборудование: Учебная мебель на 56 посадочных мест, рабочее место преподавателя, доска меловая (односекционная) - 1 шт., кафедра - 1 шт., стол - 1 шт., стул - 2 шт., Компьютер Intel Core i3-2100 CPU @ 3.10GHz/4/500 Acer V193 - 1 шт., Мультимедийный проектор Panasonic PT-VX610E - 1 шт., Мультимедийный проектор Optoma EX-632 - 1 шт., Экран DRAPER TARGA 221x295 - 1 шт. Наборы демонстрационного оборудования и учебно-наглядных пособий: мультимедийные приложения к лекционным курсам и практическим занятиям, интерактивные учебно-наглядные пособия.</p>	<p>191023, г. Санкт-Петербург, ул. Канал Грибоедова, 30/32, литер «А», «Б», «Р»</p>
<p>Ауд. 2057 лаборатория Инженерно-технической защиты, лаборатория Программно-аппаратной защиты. Специализированная мебель и оборудование: Учебная мебель на 30 посадочных мест (Парта двухместная – 11 шт., стол – 8 шт., стулья- 30 шт.); 2 рабочих места преподавателя (2 стола, 2 стула); стол – 1 шт.; трибуна для выступлений – 1 шт.; шкаф для документов – 1 шт.; стенды настенные пробковые – 2 шт.; шкаф настенный со стеклянными створками – 4 шт.; доска для маркеров двухсторонняя – 1 шт.; персональный компьютер IBM PC-совместимый (i5-3470/RAM 8Gb/HDD 500Gb/Win7pro) – 7 шт.; персональный компьютер IBM PC-совместимый (i3-2100/RAM 8Gb/HDD 500Gb/Win7pro) – 8 шт.; коммутатор Cisco для организации локальной сети лаборатории с подключением к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации – 1 шт.; шкаф серверный 42U – 1 шт.; шкаф телекоммуникационный 20U – 1 шт.; проектор NEC ME-401X – 1 шт.; экран для проектора Screen Media Goldview 244*244MW настенный – 1шт.; акустическая система марка Microlab модель Pro2– 1 шт.; коммутатор консольный Trend Net TK-803R – 1 шт.; разветвитель видеосигнала Aten VS-92A – 1 шт.; лабораторный стенд НПП «Учтех-Профи» «ОЭ-МР» – 1 шт.; лабораторный стенд НПП «Учтех-Профи» «ОЦТ-МР» – 1 шт.; лабораторный стенд НПП «Учтех-Профи» «ФОЭ-НР» – 1 комплект; комплект плакатов НПП «Учтех-Профи» – 1 шт.; генератор акустического шума ЛГШ-301 АО «Лаборатория ПППШ» – 1 шт.; виброгенератор ЛГШ-403 в комплекте с вибропреобразователями ЛВП-2о, ЛВП-2Т АО «Лаборатория ПППШ» – 1 шт.; фильтр сетевой однофазный ЛФС-10-1Ф АО «Лаборатория</p>	<p>191023, г. Санкт-Петербург, ул. Канал Грибоедова, 30/32, литер «А», «Б», «Р»</p>

<p>ППШ» – 1 шт.; генератор шума по цепям электропит., заземл. и ПЭМИ ЛГШ-503 АО «Лаборатория ППШ» – 1 шт.; устройство защиты телефонных линий Гранит-8 абонентское АО «Лаборатория ППШ» – 1 шт.; сервер HP-DL – 5 шт.; Коммутатор Cisco Small Business SF302-08 – 4 шт.; Коммутатор Cisco 2950 – 3 шт.; Коммутатор Cisco 3560 – 1 шт.; Беспроводной маршрутизатор TP-Link TL-WR941 ND; Электронные ключи Guardant – 16 шт.; огнетушитель ОУ-5 – 1 шт.; огнетушитель ОП-4(3)-BCE – 1 шт. Наборы демонстрационного оборудования и учебно-наглядных пособий: мультимедийные приложения к лекционным курсам и практическим занятиям, интерактивные учебно-наглядные пособия.</p>	
<p>Ауд. 2034 Компьютерный класс (для проведения практических занятий, курсового проектирования (выполнения курсовых работ) с применением вычислительной техники). Оборудован мультимедийным комплексом. Специализированная мебель и оборудование: Учебная мебель на 25 посадочных мест, рабочее место преподавателя (стол 1шт., кресло 1шт.), доска маркерная 1 шт., вешалки стойки 2шт., стульев 3шт. Компьютер I5-7400/8Gb/1Tb/DELL S2218H - 21 шт., Сетевой коммутатор Cisco WS-C2960-48TT-L (Catalyst2960) 48портов 10/100Мбит/с+2п - 1 шт., Коммутатор Cisco Catalyst 2960 24 WS-C2960-24PC-L - 1 шт. Наборы демонстрационного оборудования и учебно-наглядных пособий: мультимедийные приложения к лекционным курсам и практическим занятиям, интерактивные учебно-наглядные пособия.</p>	<p>191023, г. Санкт-Петербург, ул. Канал Грибоедова, 30/32, литер «А», «Б», «Р»</p>
<p>Ауд. 2021 Лаборатория "Лабораторный комплекс" Специализированная мебель и оборудование: Учебная мебель на 22 посадочных места (22 компьютерных стола, черных кресел 22шт.) Учебная мебель на 42 посадочных мест (парт 21 шт.) рабочее место преподавателя (компьютерный стол 1шт.) доска, меловая 3-х секционная 1шт., доска маркерная на колесиках 1 шт., часы 1 шт., кафедра 1шт., стол 1шт., тумбочка 1шт., стул из 4шт., вешалка стойка 2шт., жалюзи 3шт. Компьютер i5-8400/8GB/500GB_SSD/Viewsonic VA2410-mh - 23 шт., Установка демонстрационных учебных фильмов - 1 шт., Компьютер в комплектации системный блок Intel pentium x2 g3250 клавиатура+мышь L (жесткий диск 500gb, монитор philips 21.5') - 1 шт. Наборы демонстрационного оборудования и учебно-наглядных пособий: мультимедийные приложения к лекционным курсам и практическим занятиям, интерактивные учебно-наглядные пособия.</p>	<p>191023, г. Санкт-Петербург, ул. Канал Грибоедова, 30/32, литер «А», «Б», «Р»</p>

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩЕГОСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Приступая к изучению дисциплины, обучающемуся необходимо ознакомиться со следующими документами:

- учебно-методической документацией;
- локальными нормативными актами, регламентирующими основные вопросы организации и осуществления образовательной

деятельности, в том числе регламентирующие порядок проведения текущего контроля успеваемости и промежуточной аттестации обучающихся;

– графиком консультаций сотрудников профессорско-преподавательского состава.

Уровень и глубина освоения дисциплины определяются активной и систематической работой обучающихся на лекционных занятиях, занятиях семинарского типа, выполнением самостоятельной работы, в том числе в части выделения наиболее значимых и актуальных проблем для дальнейшего изучения. Особым условием качественного освоения дисциплины является эффективная организация труда, позволяющая распределить учебную нагрузку равномерно в соответствии с графиком учебного процесса.

При подготовке к учебным занятиям обучающимся предоставляется возможность посещения консультаций сотрудников профессорско-преподавательского состава СПбГЭУ согласно расписанию, установленному в графике консультаций.

Аудиторная и внеаудиторная работа обучающихся должна быть направлена на формирование:

- фундаментальных основ мировоззрения обучающихся и естественнонаучного познания;
- базисных знаний, соответствующих направлению подготовки и заявленной профессиональной области, формирующих целевую и профессиональную основу для подготовки кадров;
- профессиональных компетенций ориентированных на удовлетворение потребностей рынка труда;
- индивидуальной траектории посредством освоения уникального набора профессиональных компетенций дополняющих компетентностную модель обучающегося, за счет ориентации на конкретные профессиональные специализированные области знаний, определяемые представителями рынка труда;
- метанавыков обучающихся, таких как: командная работа и лидерство, анализ данных, цифровые навыки, разработка и реализация проектов, межкультурное взаимодействие.

8. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Обучение обучающихся с ограниченными возможностями здоровья при необходимости осуществляется на основе адаптированной рабочей программы с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося).

В целях освоения учебной программы дисциплины инвалидами и лицами с ограниченными возможностями здоровья Университет обеспечивает:

- для инвалидов и лиц с ограниченными возможностями здоровья по зрению: размещение в доступных для обучающихся, являющихся слепыми или слабовидящими, местах и в адаптированной форме справочной информации о расписании учебных занятий; присутствие ассистента, оказывающего обучающемуся необходимую помощь; выпуск альтернативных форматов методических материалов (крупный шрифт или аудиофайлы);

- для инвалидов и лиц с ограниченными возможностями здоровья по слуху: надлежащими звуковыми средствами воспроизведение информации;

- для инвалидов и лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата: возможность беспрепятственного доступа обучающихся в учебные помещения, туалетные комнаты и другие помещения кафедры, а также пребывание в указанных помещениях.

Обучающиеся из числа инвалидов и лиц с ОВЗ обеспечены печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья. Образование обучающихся с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах или в отдельных организациях.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

1.1 Контрольные вопросы и задания к промежуточной аттестации

- 1 Общие сведения о технологии терминального доступа. Обеспечение безопасности сервера ОС Windows Server 2016.
- 2 Служба каталогов LDAP. Система единого входа в сеть на основе протокола Kerberos. Создание единого пространства безопасности на базе Active Directory.
- 3 Защита средствами файловых систем ОС Windows и Linux.
- 4 Цели и задачи аудита безопасности. Этапы и методы проведения, результаты работ.
- 5 Нормативно-правовые и организационные основы проведения аудита безопасности компьютерных систем
- 6 Применение средств автоматизации комплексного аудита информационной безопасности.
- 7 Структура и функции комплексных экспертных систем аудита безопасности.
- 8 Резервное копирование данных. Виды, достоинства и недостатки.
- 9 Архивирование в Windows Server 2016.
- 10 Основные подходы к построению защищенных операционных систем.
- 11 Требования к безопасности ОС согласно ISO/МЭК.
- 12 Технические методы и средства защиты ПО.
- 13 Средства безопасности ОС Windows.
- 14 Средства безопасности ОС Linux.
- 15 Виды резервного копирования.
- 16 Провести резервное копирование системного диска в ОС Windows 2016.
- 17 Настройка дискреционного доступа к данным в Astra Linux.
- 18 Настройка мандатного доступа к данным в Astra Linux.
- 19 Провести шифрование дисков в ОС Windows с помощью утилиты BitLocker.
- 20 Настроить аутентификацию по протоколу Kerberos.
- 21 Настроить аутентификацию по протоколу NTLM.
- 22 Настроить политику аудита в ОС Windows 2016.
- 23 Доступ к файлам и каталогам в ФС Ext4.
- 24 Доступ к файлам и каталогам в ФС NTFS.
- 25 Защита в ФС накопителей SSD.

1.2 Темы письменных работ

Рабочей программой дисциплины не предусмотрено.

1.3 Контрольные точки

Номер контрольной точки	Тип контрольной точки	Способ проведения	Номера тем
1	Индивидуальное задание	с помощью технических средств и информационных систем	1-2
2	Тест	с помощью технических средств и информационных	1-6

		систем	
3	Текущий контроль	с помощью технических средств и информационных систем	1-6

1.4 Другие объекты оценивания

Рабочей программой дисциплины не предусмотрено.

1.5 Самостоятельная работа обучающегося

Наименования самостоятельной работы	Номера тем
Подготовка к лекционным и практическим занятиям	1-6
Выполнение домашних заданий	1-6
Подготовка к экзамену	1-6

1.6 Шкала оценивания результата

Шкалы оценивания и процедуры оценивания результатов обучения **по дисциплине** регламентируются Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся по программам высшего образования и Положением о балльно-рейтинговой системе. Для оценки сформированности результатов обучения по дисциплине используется **балльно-рейтинговая система успеваемости обучающихся**:

Формой итогового контроля по дисциплине является экзамен (или дифференцированный зачет), итоговая оценка формируется в соответствии со шкалой, приведенной ниже в таблице:

Баллы	Оценка
≤ 54	неудовлетворительно
55-69	удовлетворительно
70-84	хорошо
≥ 85	отлично

Шкала оценивания результата

2 (балл до 54)	Демонстрирует непонимание проблемы. Многие требования, предъявляемые к заданию не выполнены. Демонстрируется первичное восприятие материала. Работа незакончена и /или это плагиат.
3 (балл 55-69)	Демонстрирует частичное понимание проблемы. Большинство требований, предъявляемых, к заданию выполнены. Владение элементами заданного материала. В основном выполненный материал понятен и носит целостный характер.

4 (балл 70-84)	Демонстрирует значительное понимание проблемы обозначенной дисциплиной. Все требования, предъявляемые к заданию выполнены. Содержание выполненных заданий раскрыто и рассмотрено с разных точек зрения.
5 (балл 85-100)	Демонстрирует полное понимание проблемы. Все требования, предъявляемые к заданию выполнены. Продемонстрировано уверенное владение материалом дисциплины. Выполненные задания носят целостный характер, выполнены в полном объеме, структурированы, представлены различные точки зрения, продемонстрирован творческий подход.